

My Journey 私の旅

Driven by the Inspiration from Hackers in SF Novels



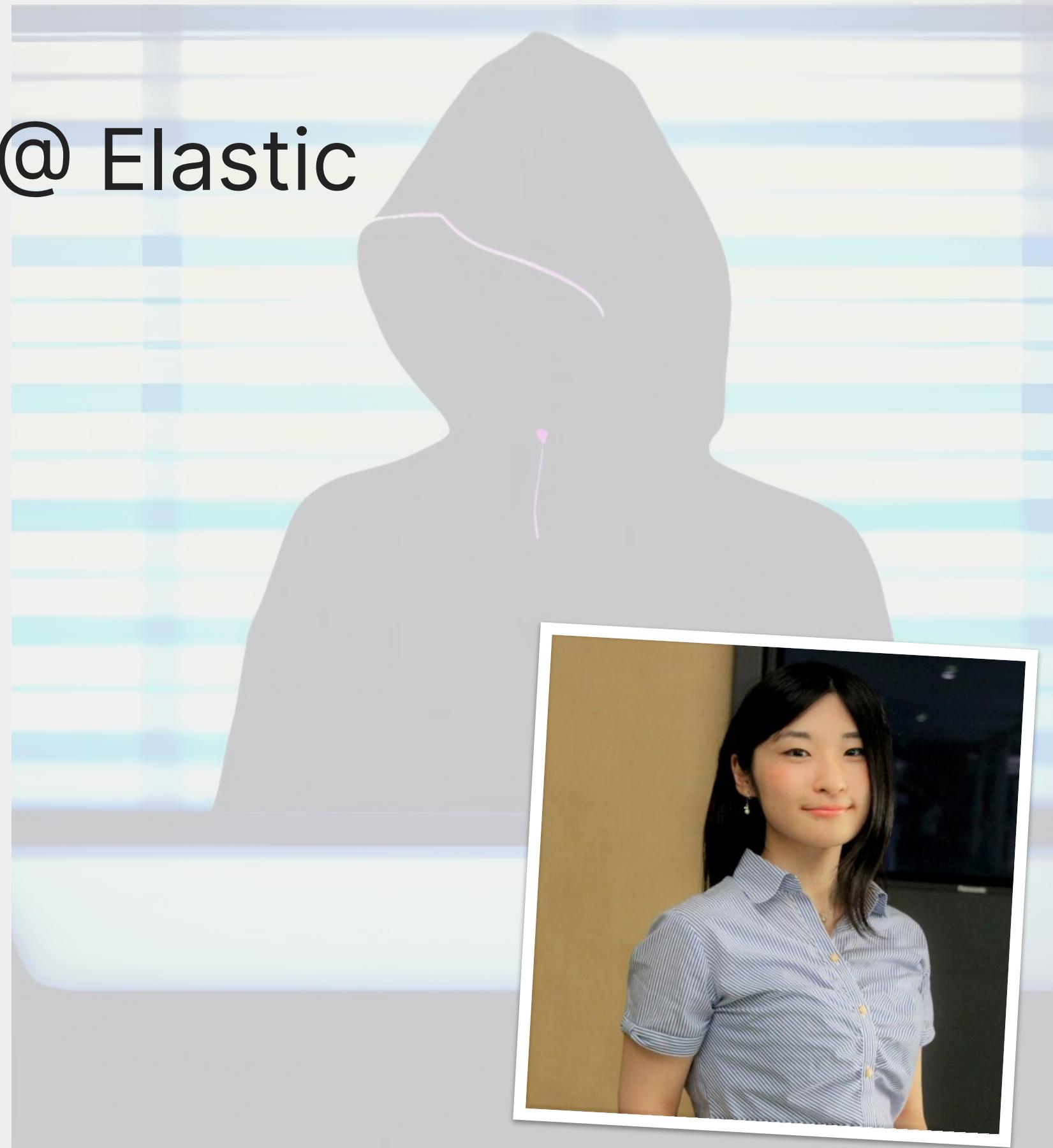
Asuka Nakajima | 中島 明日香

Security Research Engineer @ Elastic



whoami : Asuka Nakajima

■ Security Research Engineer @ Elastic



whoami : Asuka Nakajima

- Security Research Engineer @ Elastic
- 10+ years of experience in Cyber Security R&D



whoami : Asuka Nakajima

- Security Research Engineer @ Elastic
- 10+ years of experience in Cyber Security R&D
- Founded the first female infosec community in Japan



whoami : Asuka Nakajima

- Security Research Engineer @ Elastic
- 10+ years of experience in Cyber Security R&D
- Founded the first female infosec community in Japan
- BlackHat USA / Asia Review Board



whoami : Asuka Nakajima

- Security Research Engineer @ Elastic
- 10+ years of experience in Cyber Security R&D
- Founded the first female infosec community in Japan
- BlackHat USA / Asia Review Board
- Published books (best selling book!)





Why did you decide
to enter this field?





Why did you decide
to enter this field?



What motivates you?





Why did you decide
to enter this field?

What motivates you?

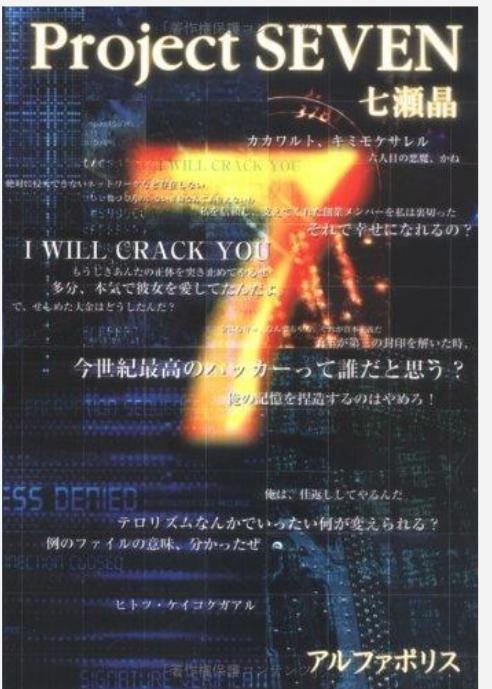
How did you
improve your
skills?

Timeline



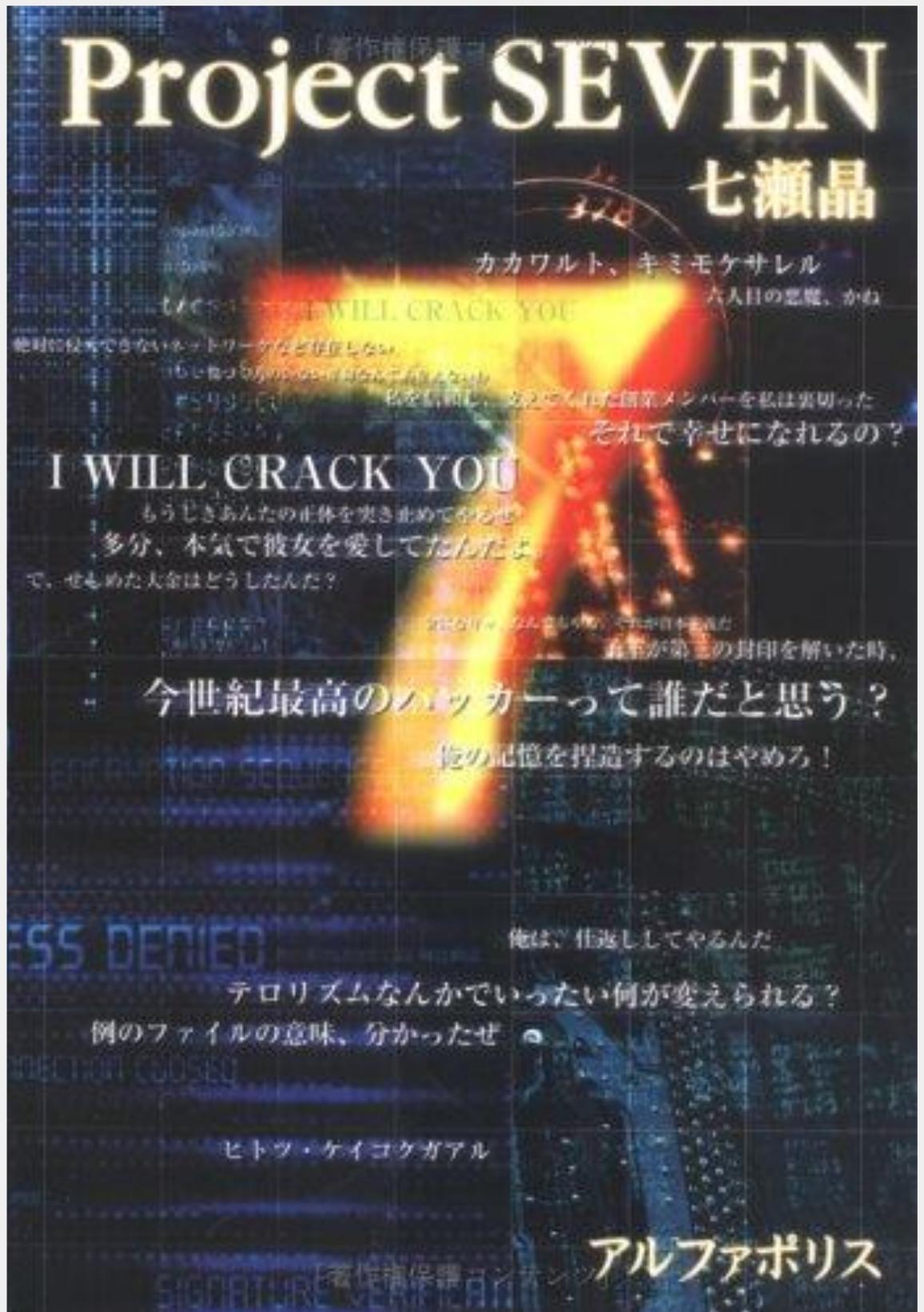
Timeline

age 14



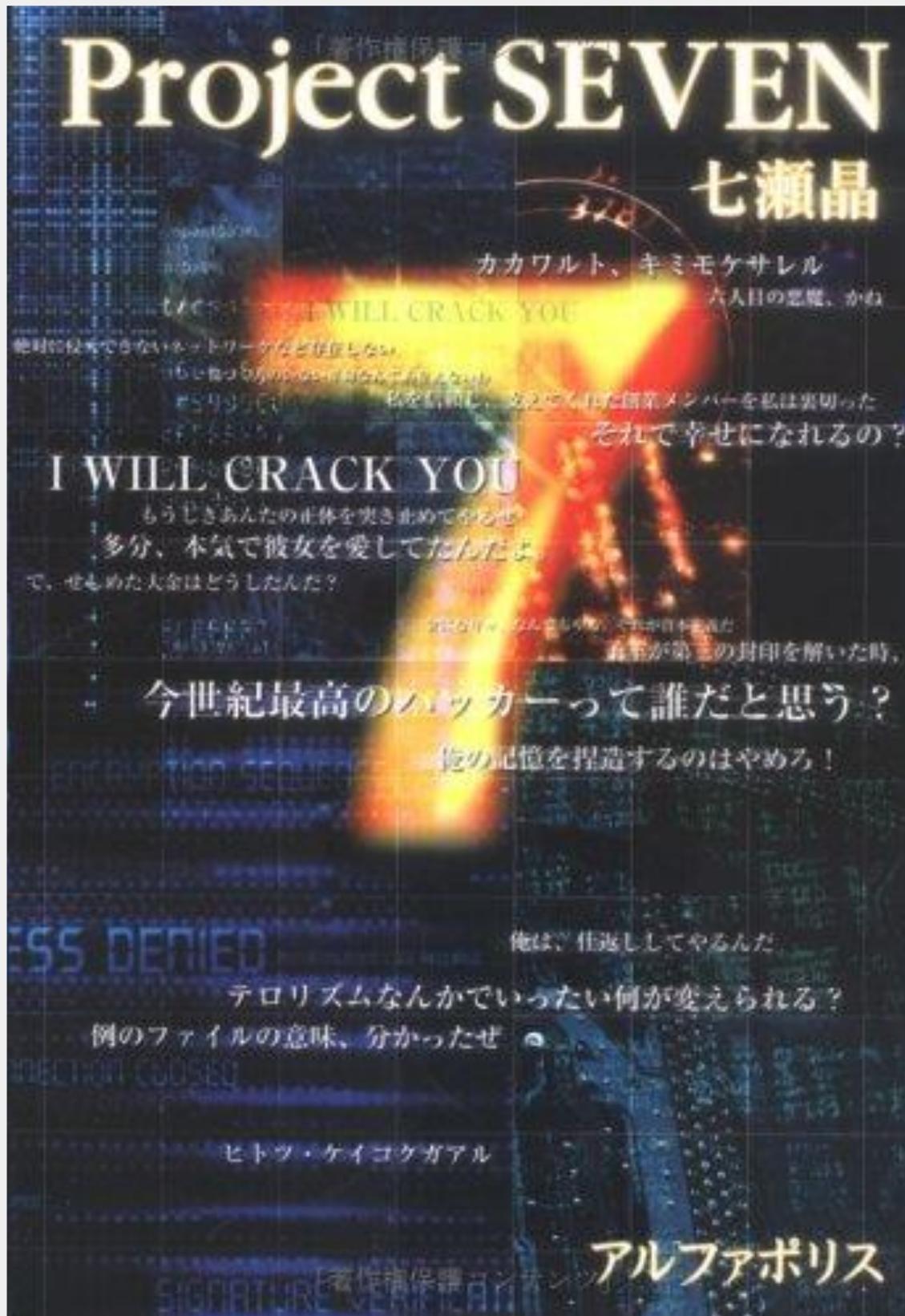
2004





<https://www.amazon.co.jp/dp/443406732X>

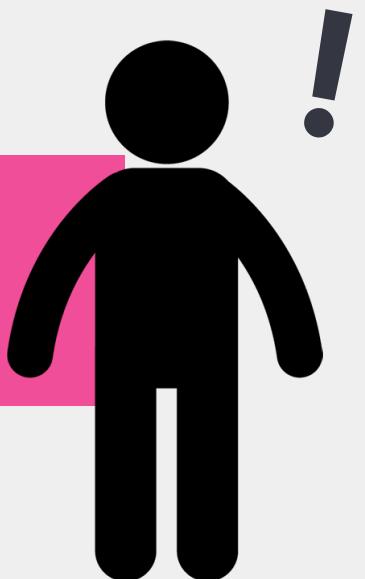
A **high school girl hacker** 
and a programmer **saving the world**  from cyber-terrorists



<https://www.amazon.co.jp/dp/443406732X>

A **high school girl hacker** 
and a programmer **saving the world**  from cyber-terrorists

Hackers are so cool!!!



Started studying computers
and security on my own



?

?

?

?

I knew almost nothing
about computers.. □

.?

?

?

?

?

?

謎

Reading a book like “How to use hacking tools” 😢



Reading a book like “How to use hacking tools” 😢



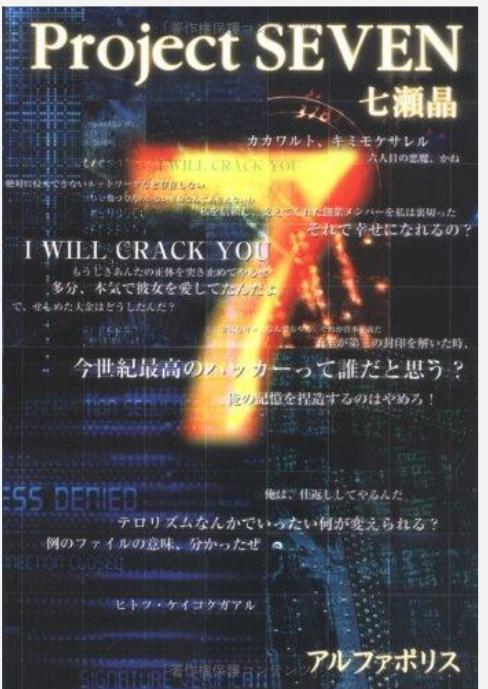
Wanted to study advanced topics, even though I didn't understand basics yet.. □

A soft-focus background image shows a person with glasses looking down at a shelf filled with books. The books are stacked in various directions, creating a sense of depth. The colors are warm and muted.

I started with studying for a beginner
level IT certification to **learn the basics**

Timeline

age 14



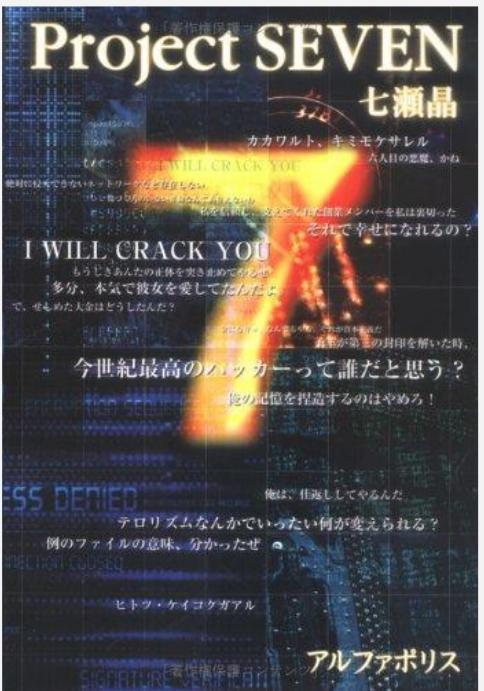
2004



Timeline

age 14

University
Days



2009

2004



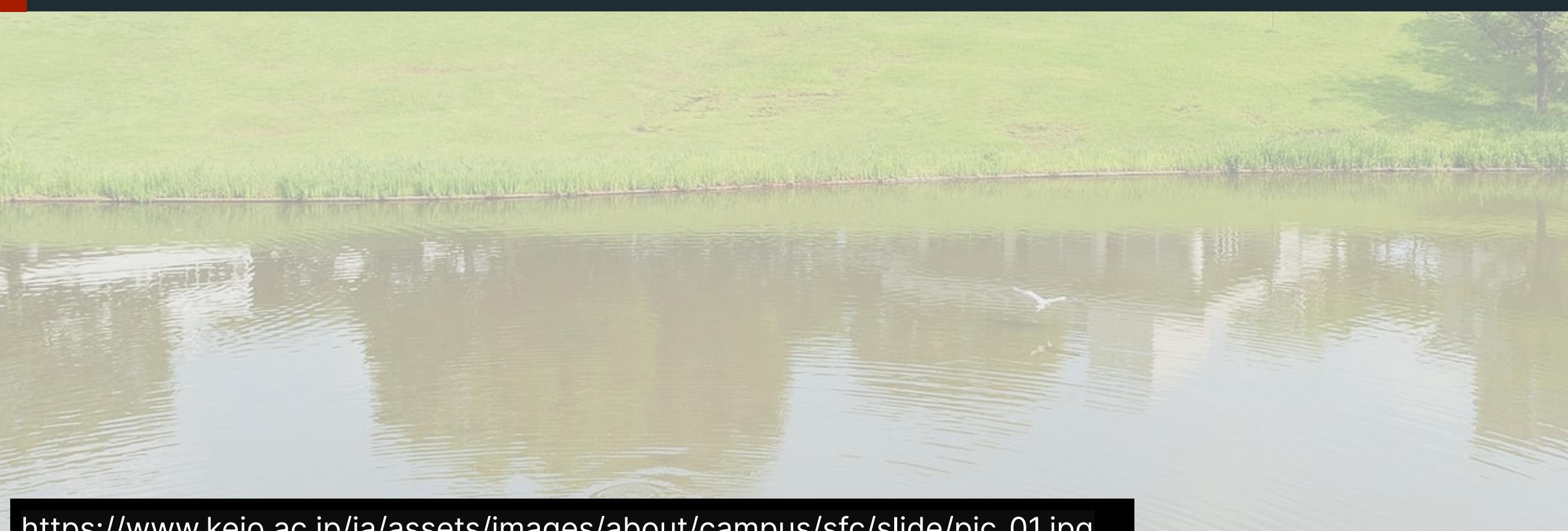
Enrolled Keio University

Belonged to the laboratory of a leading
IDS (Intrusion Detection System)
researcher in Japan



Enrolled Keio University

Belonged to the laboratory of a leading
IDS (Intrusion Detection System)
researcher in Japan



Participated Security Camp

Multi-day group training programs
for selected students throughout Japan

集え、コンピュータの未来を守るIT戦士たち。
セキュリティ&プログラミングキャンプ2009

4泊5日 交通費・宿泊費を含め、無料です。

2009.08.12 - 08.16

参加資格：22歳以下の学生・生徒

主催 独立行政法人情報処理推進機構/IPA、セキュリティ&プログラミングキャンプ・コンソーシアム
(財団法人日本情報処理開発協会/JIPDEC、NPO日本ネットワークセキュリティ協会/JNSA)

共催 経済産業省 後援 文部科学省

mp2009

ホーム

Connected with people
who are interested in security!

→キャラバン2009はこちら
Security & Programming
Camp 2009

Joined a CTF team: **sutegoma2**



DEF CON CTF Finals

Las Vegas, 2011





#2

I couldn't solve any of the challenges



#2

I couldn't solve any of the challenges 😢



#2

Even though I had passed Japan's most difficult information security national qualification, **there was so much I didn't know** 😱



Understood the World Class Level



and, realized that I was quite far from the top level...



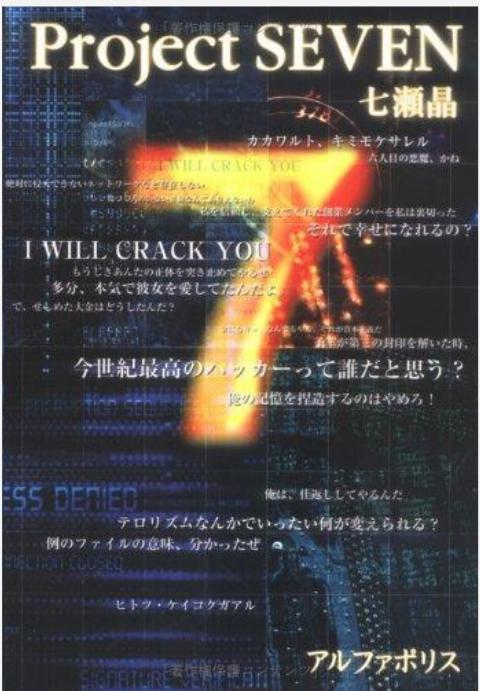
Top level
is .. there?!

Me

Timeline

age 14

University
Days



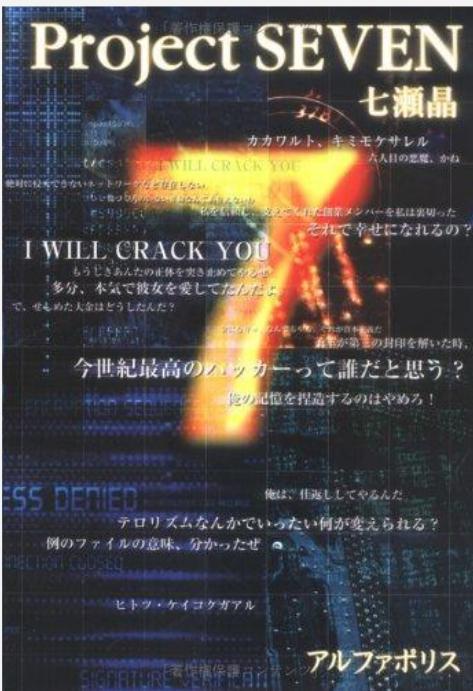
2009

2004



Timeline

age 14



2004

University
Days



Vuln
Research



2013



Started my career as a
Security Researcher



Software Vulnerability Research



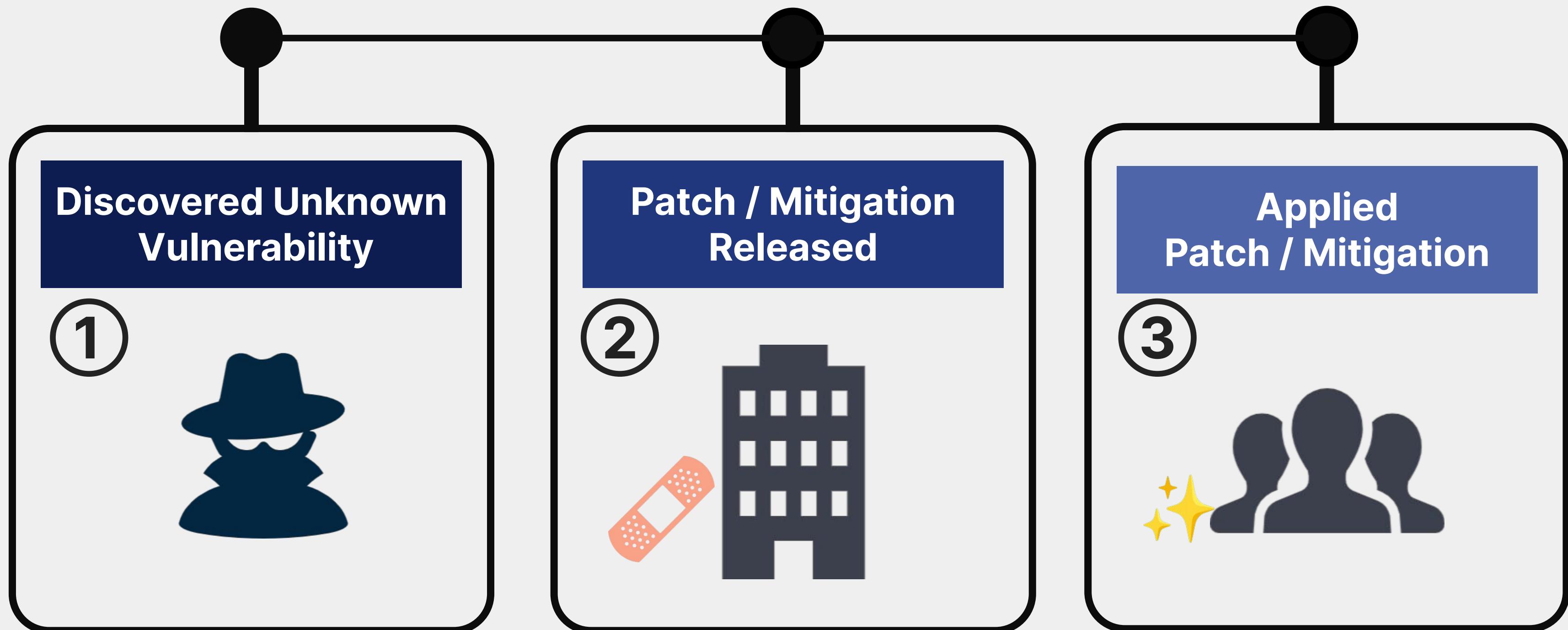
Software Vulnerability Research

If I can **find and address** **vulnerabilities**  in widely-used software before attackers can exploit, it might **help save the world?** 

One-Day Vulnerability

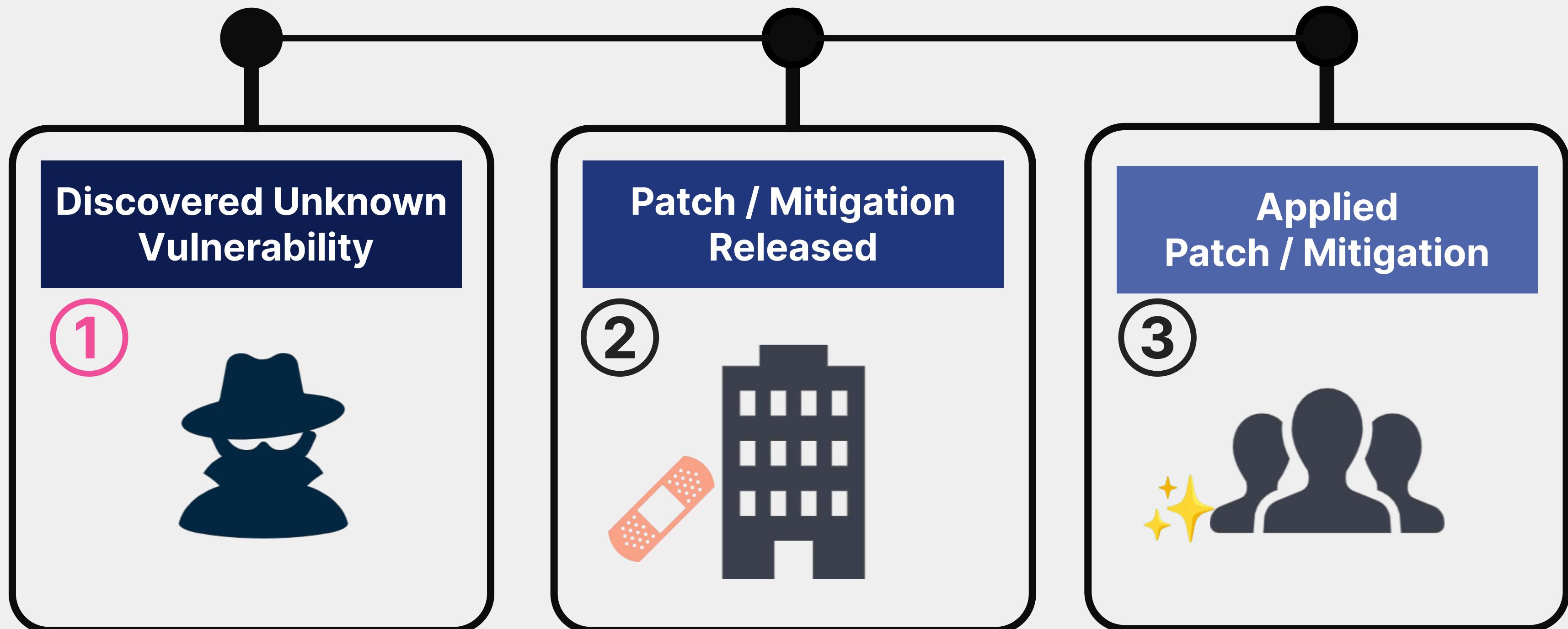
One-day Vulnerability

aka N-day Vulnerability



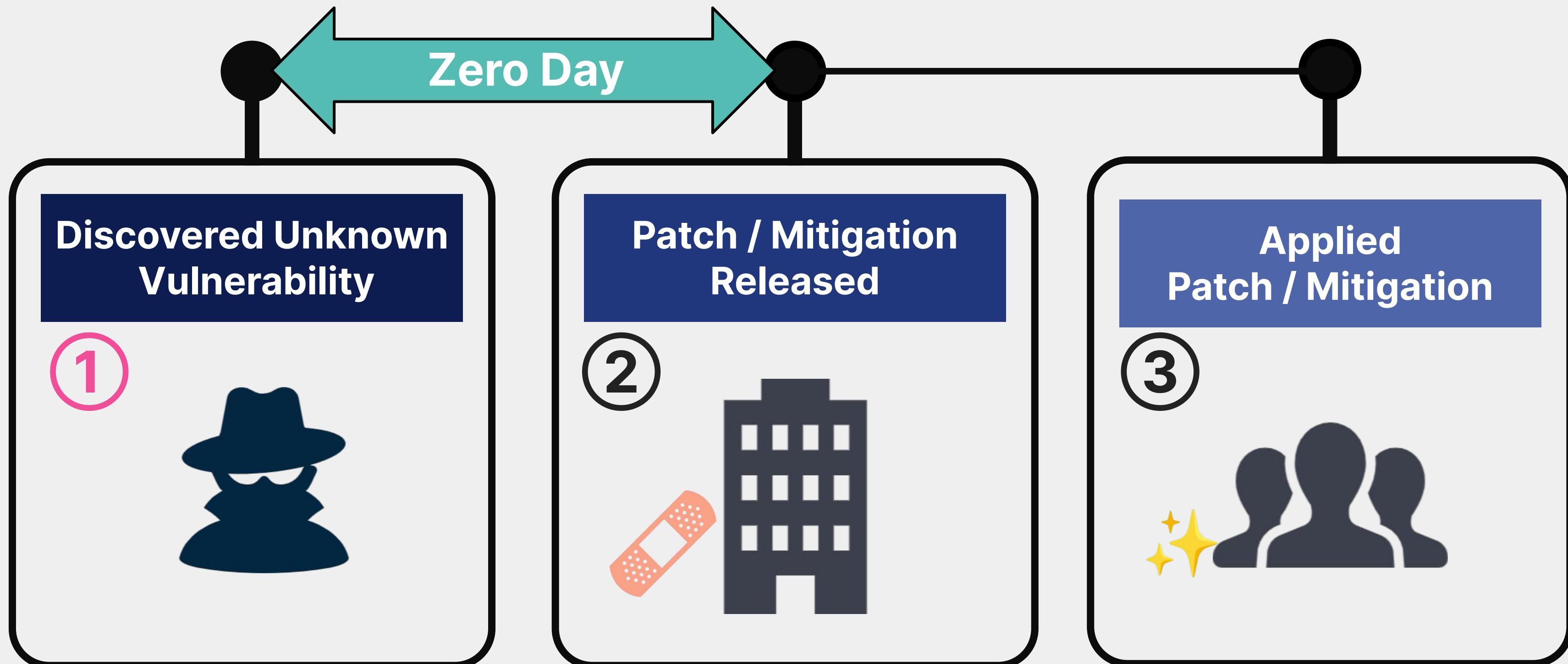
One-day Vulnerability

aka N-day Vulnerability



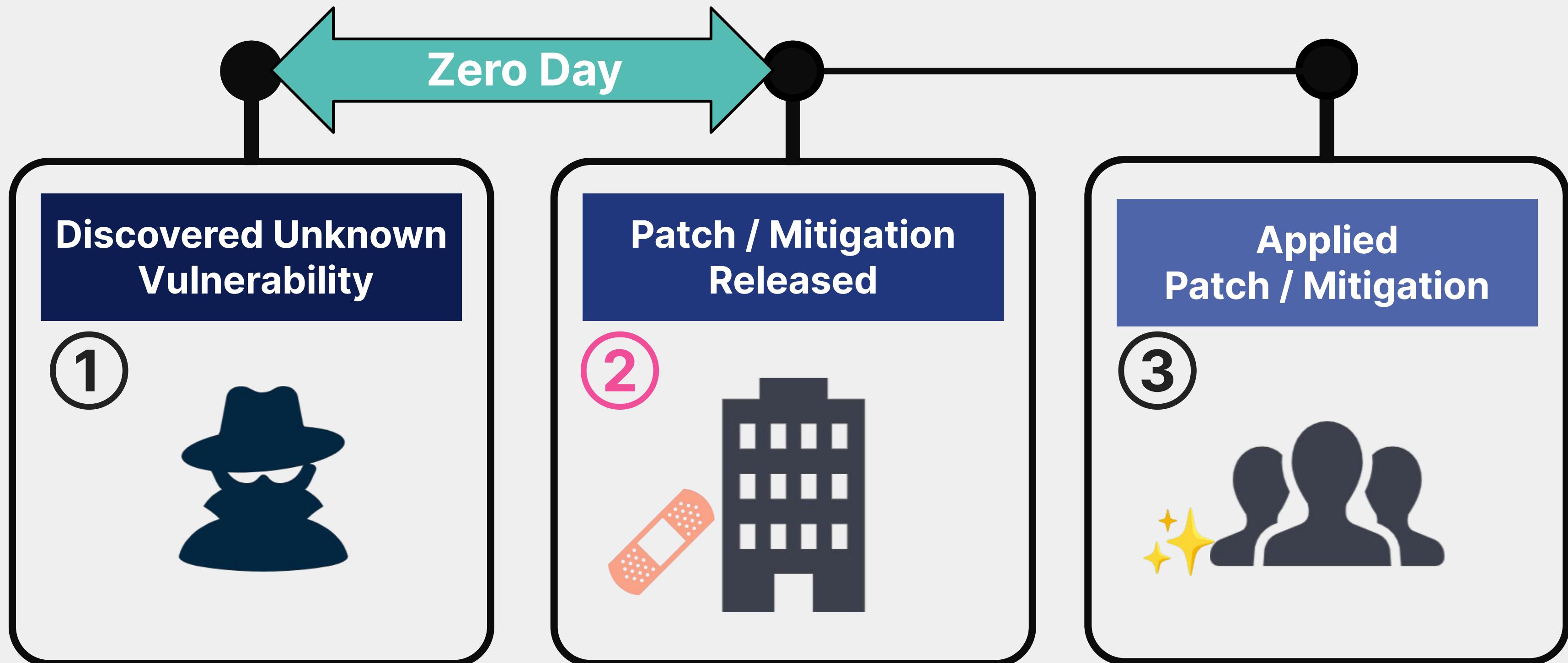
One-day Vulnerability

aka N-day Vulnerability



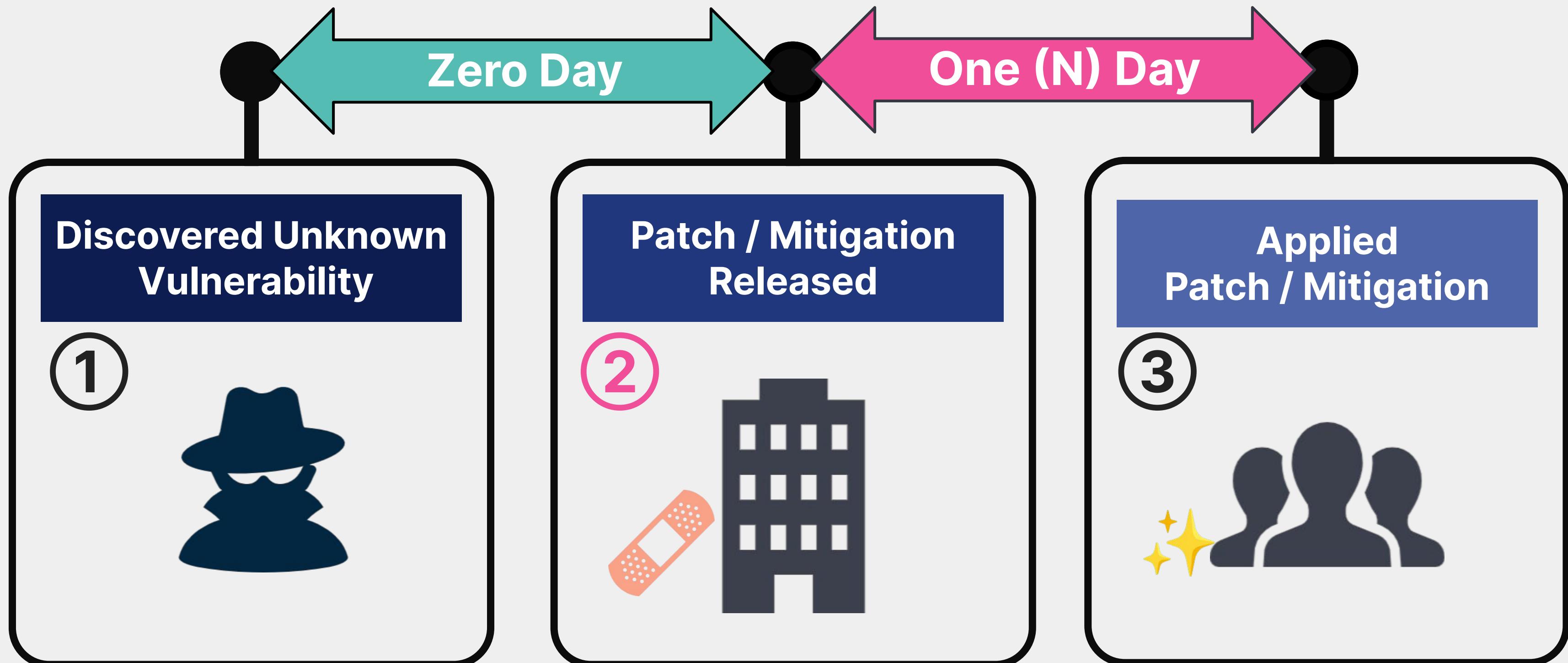
One-day Vulnerability

aka N-day Vulnerability



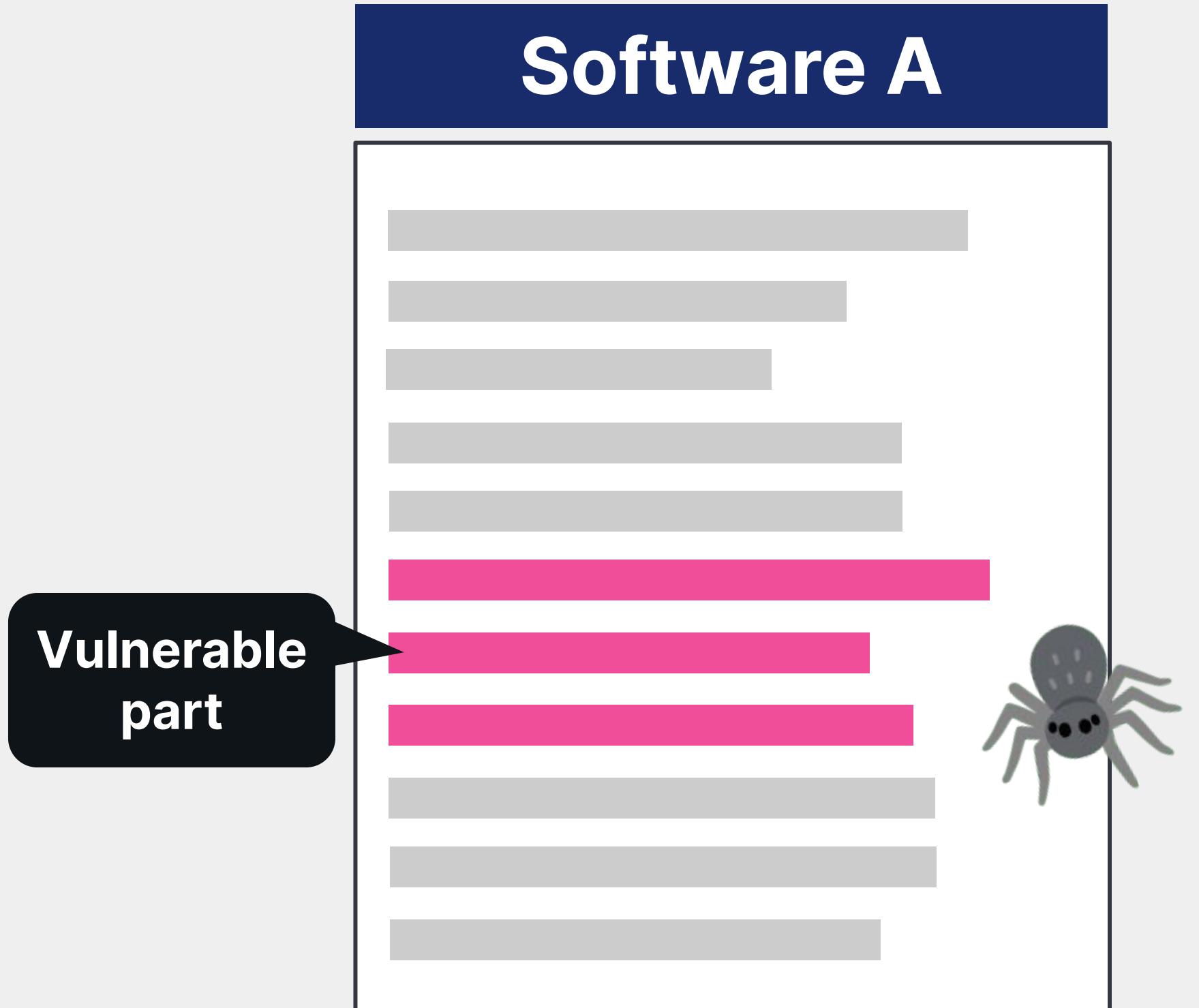
One-day Vulnerability

aka N-day Vulnerability

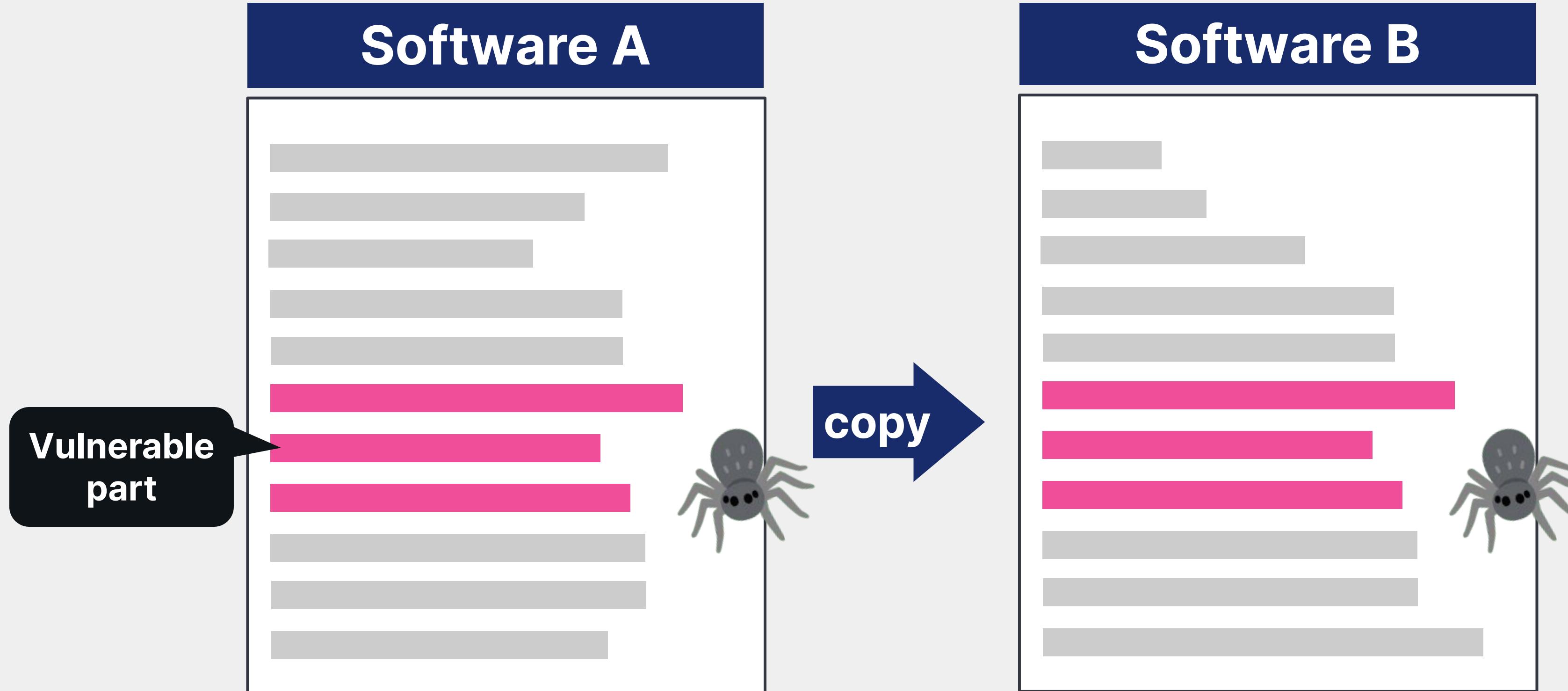


Code Clone Vulnerability

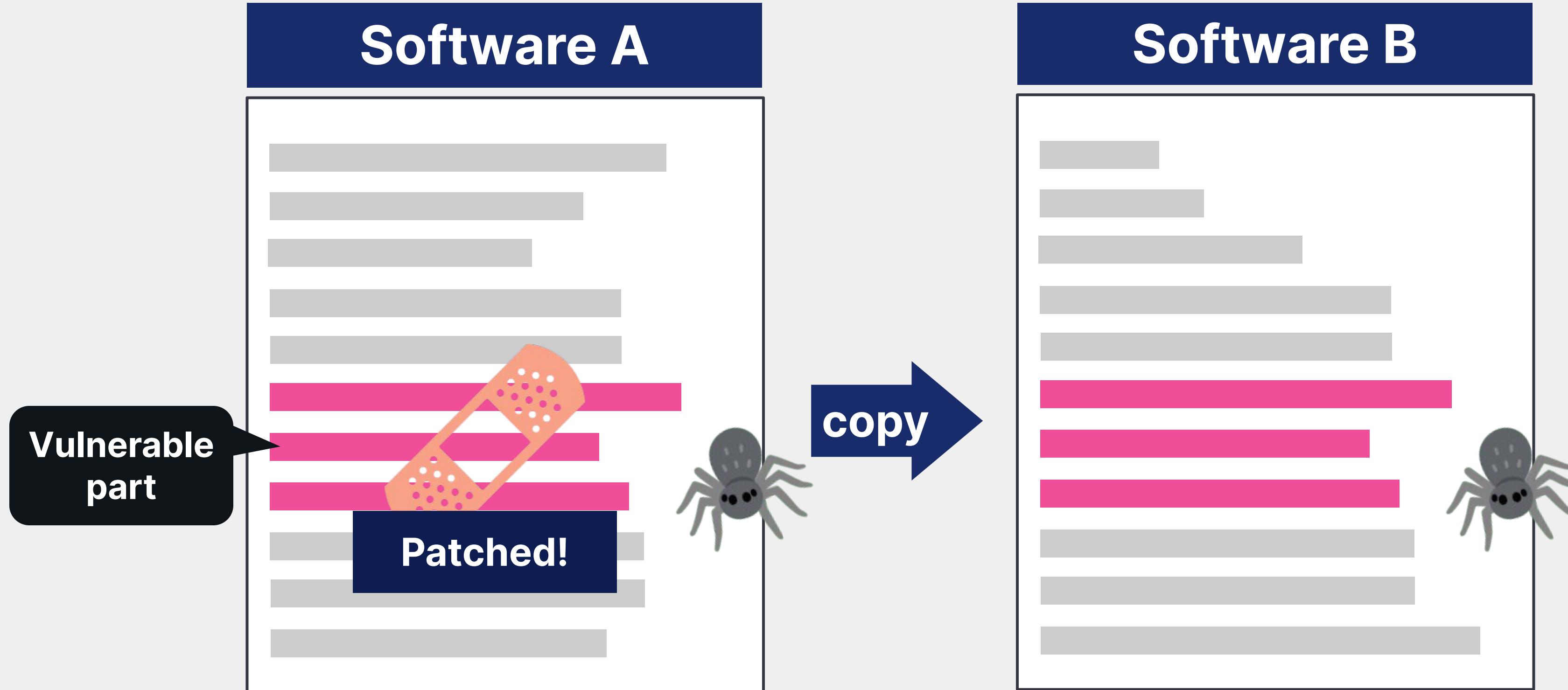
Code Clone Vulnerability



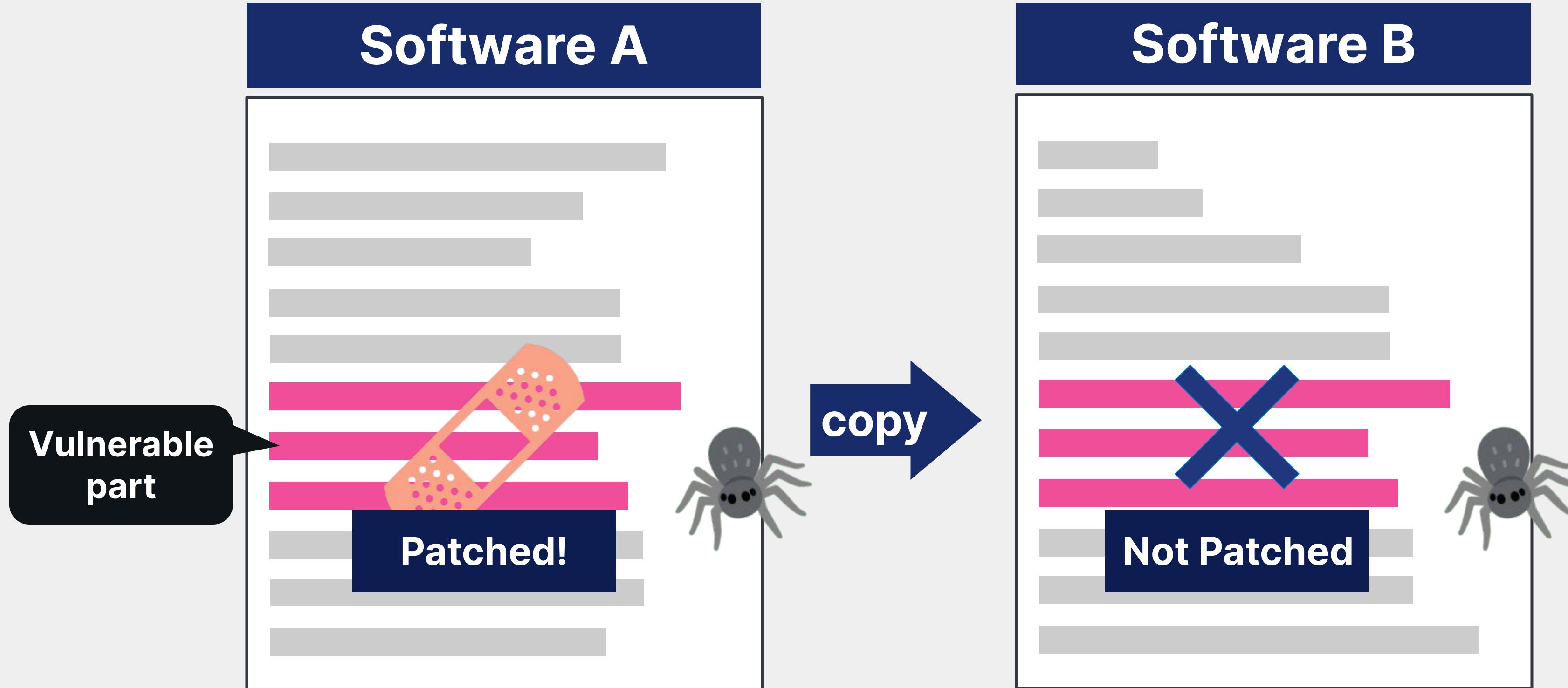
Code Clone Vulnerability



Code Clone Vulnerability



Code Clone Vulnerability



Cloned Vulnerabilities Might Not be Fixed

Why does it Happen?

Why does it Happen?

Copy & Paste

Ctrl + C

Ctrl + V

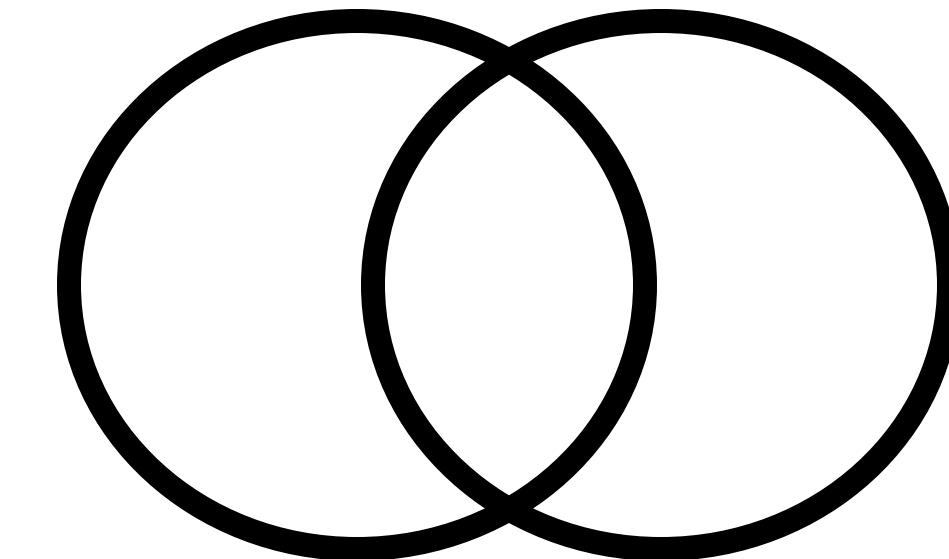
Why does it Happen?

Copy & Paste

Ctrl + C

Ctrl + V

Source Code Sharing



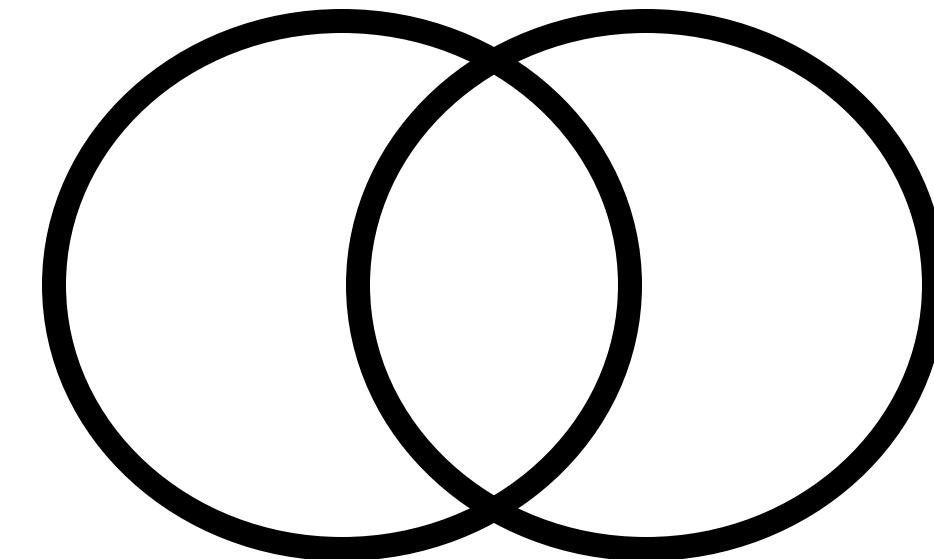
Why does it Happen?

Copy & Paste

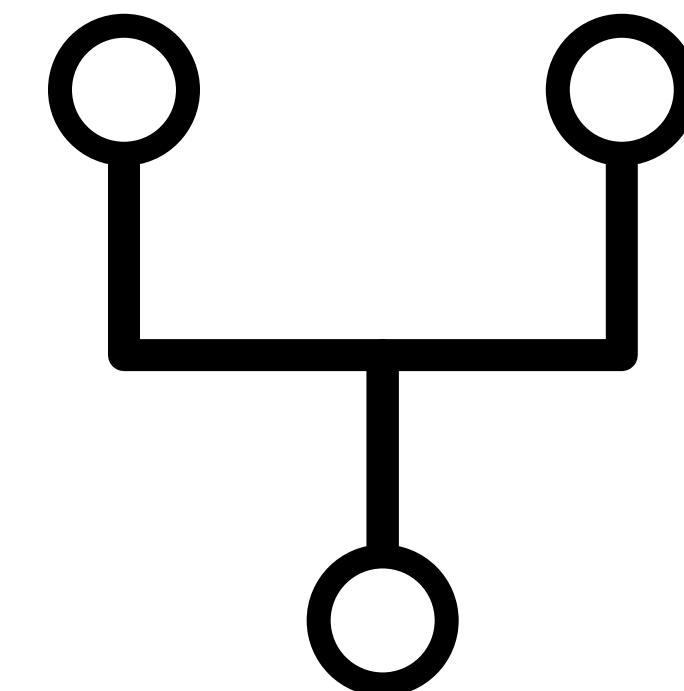
Ctrl + C

Ctrl + V

Source Code Sharing



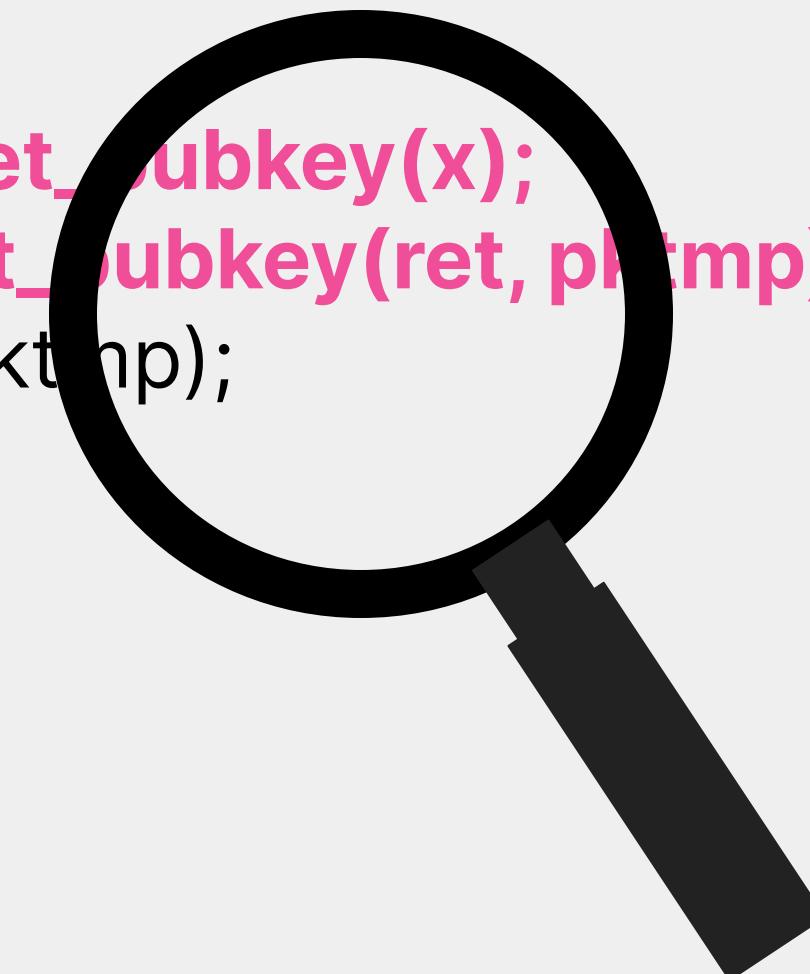
Fork



Code Clone Search (2014)

```
pkttmp = X509_get_subkey(x);
i = X509_REQ_set_subkey(ret, pkttmp);
EVP_PKEY_free(pkttmp);
```

.....



Source Code Based

```
00:00E0 52 69 63 68 27 35 39 26-00 00 00 00 00 00 00 00 00 00  
00:00F0 50 45 00 00 4C 41 05 00-03 B4 77 E0 00 00 00 00 00  
00:0100 00 00 00 00 00 E0 00 22 01-0B 01 0A 00 00 32 04 00  
00:0110 00 20 02 00 00 00 00 00 00 00-CC.....
```



Binary Based

Code Clone Search (2014)

```
pkttmp = X509_get_subkey(x);
i = X509_REQ_set_subkey(ret, pkttmp);
EVP_PKEY_free(pkttmp);
```

.....

Source Code Based

```
00:00E0 52 69 63 68 27 35 39 26-00 00 00 00 00 00 00 00  
00:00F0 50 45 00 00 4C 41 05 00-03 B4 77 E0 00 00 00 00 00  
00:0100 00 00 00 00 00 E0 00 22 01-0B 01 0A 00 00 32 04 00  
00:0110 00 20 02 00 00 C0 00 00 00-CC.....
```

Binary Based

Code Clone Search (2014)

pkttmp = X509_get_subkey(x);

Found multiple codeclone vulnerabilities! 😱

Source Code Based

Binary Based

Found a Code Clone Vulnerability in Windows!

| Original | Copy |
|---|--|
| <pre>text:11071B40 text:11071B40 public X509_cmp_time text:11071B40 proc near text:11071B40 text:11071B40 text:11071B40 var_44 = dword ptr -44h text:11071B40 var_40 = dword ptr -40h text:11071B40 var_3C = dword ptr -3Ch text:11071B40 var_34 = dword ptr -34h text:11071B40 var_30 = dword ptr -30h text:11071B40 var_2C = dword ptr -2Ch text:11071B40 var_28 = byte ptr -28h text:11071B40 var_1C = byte ptr -1Ch text:11071B40 var_1B = byte ptr -1Bh text:11071B40 var_4 = dword ptr -4 text:11071B40 arg_0 = dword ptr 4 text:11071B40 arg_4 = dword ptr 8 text:11071B40 text:11071B40 mov eax, 44h text:11071B45 call __alloca_probe text:11071B4A mov eax, __security_cookie text:11071B40 text:11071B68 text:11071B6B cmp edi, 17h text:11071B6D jnz short loc_11071BA8 text:11071B70 add ecx, 0FFFFFFF5h text:11071B73 cmp ecx, 6 text:11071B75 text:11071B77 text:11071B7A text:11071B7E text:11071B82 mov word ptr [esp+50h+var_2C], cx</pre> | <pre>.text:1009D790 .text:1009D790 sub_1009D790 .proc near ; CODE XREF: sub_1009D790+8A↓ .text:1009D790 .text:1009D790 var_44 = dword ptr -44h .text:1009D790 var_40 = dword ptr -40h .text:1009D790 var_3C = dword ptr -3Ch .text:1009D790 var_38 = dword ptr -38h .text:1009D790 var_34 = qword ptr -34h .text:1009D790 var_2C = dword ptr -20h .text:1009D790 var_28 = byte ptr -28h .text:1009D790 var_1C = byte ptr -1Ch .text:1009D790 var_1B = byte ptr -1Bh .text:1009D790 var_4 = dword ptr -4 .text:1009D790 arg_0 = dword ptr 4 .text:1009D790 arg_4 = dword ptr 8 .text:1009D790 .text:1009D790 mov eax, 44h .text:1009D795 call __alloca_probe .text:1009D790 .text:1009D795 .text:1009D79A .text:1009D79F .text:1009D7A1 .text:1009D7A5 .text:1009D7A6 .text:1009D7AA .text:1009D7AB .text:1009D7AF .text:1009D7B0 .text:1009D7B3 .text:1009D7B5 .text:1009D7B8 .text:1009D7BB .text:1009D7BD .text:1009D7CB .text:1009D7D1 .text:1009D7D1 mov eax, [esi+8] cmp edi, 17h jnz short loc_1009D7EF add ecx, 0FFFFFFF5h loc_1009D7DB eax+8] [esp+50h+var_2C+2] movq xmm0, qword ptr [eax]</pre> |
| <p>OpenSSL Library (libeay32.dll)</p> | <p>Windows (JunosPulseVpnBg.dll)</p> |

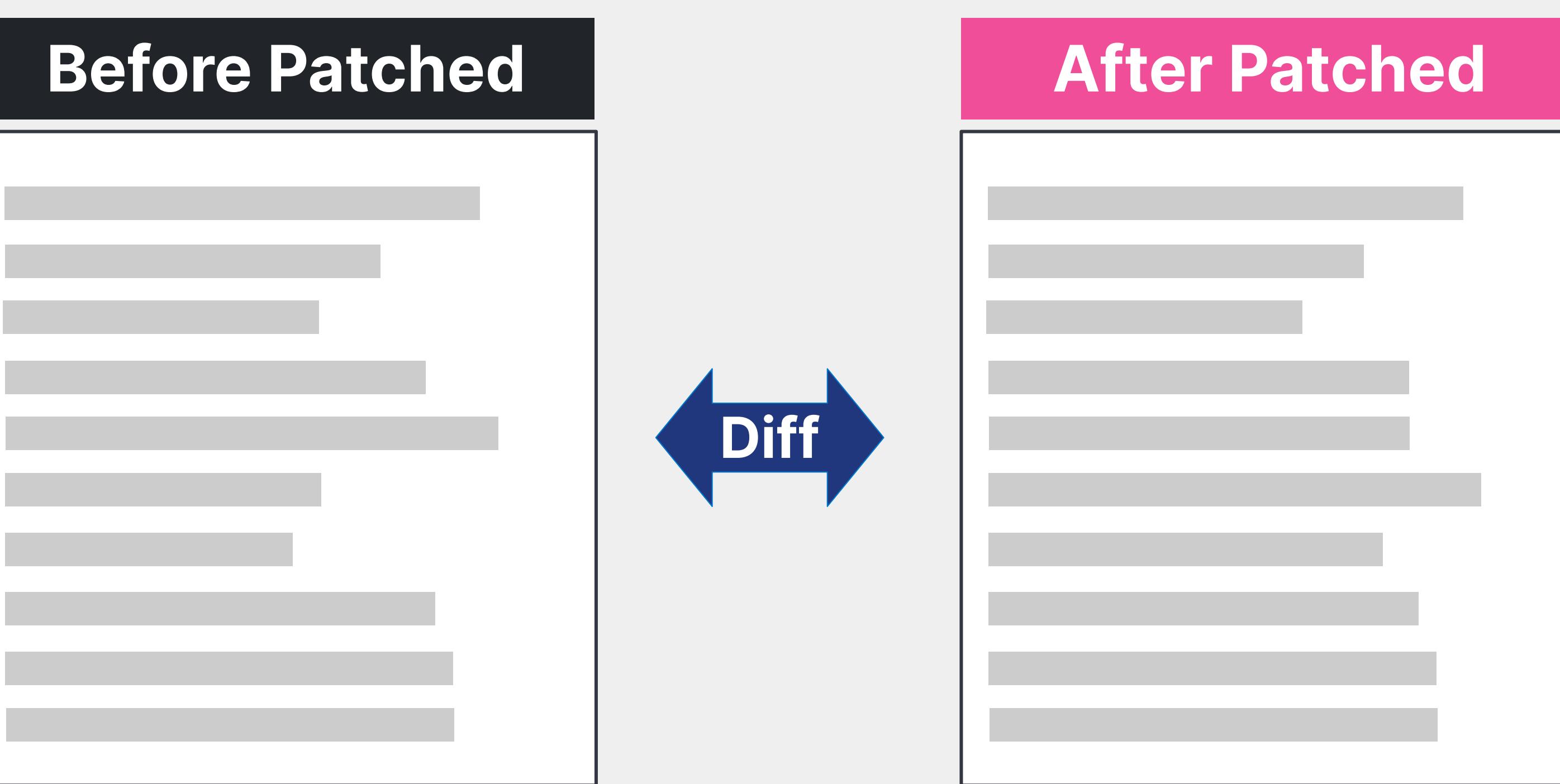
CVE-2015-1789

Positive Hack Days



Patch Diffing Manually to Find the Original Vuln Part

Patch Diffing Manually to Find the Original Vuln Part



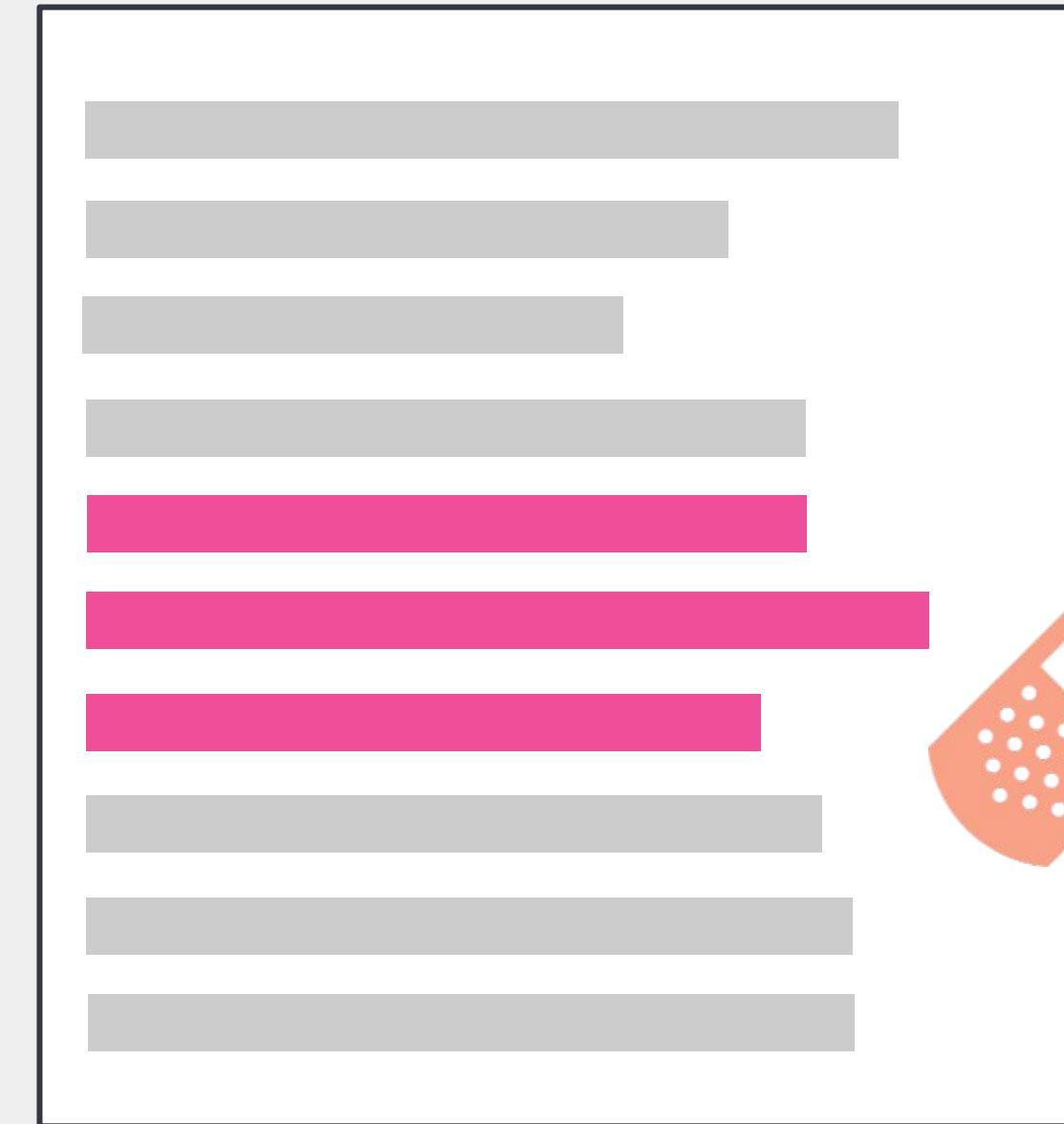
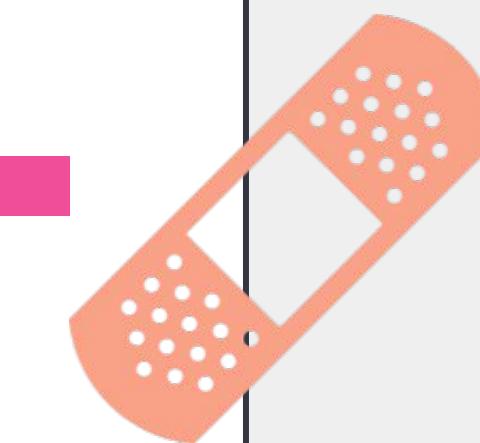
Patch Diffing Manually to Find the Original Vuln Part

Before Patched



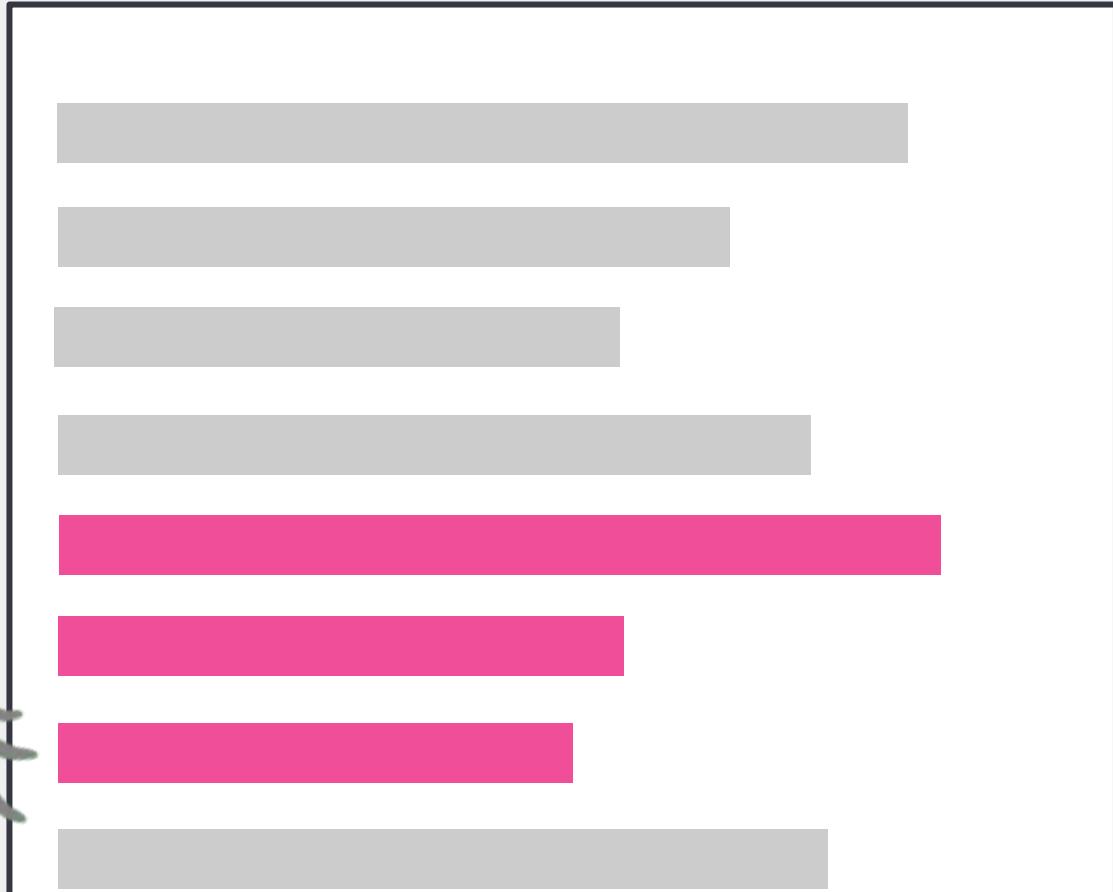
Diff

After Patched



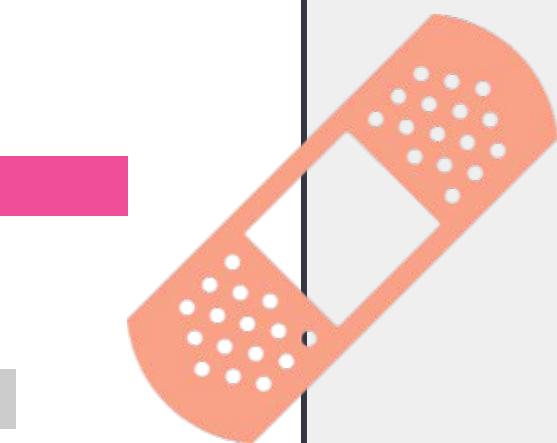
Patch Diffing Manually to Find the Original Vuln Part

Before Patched



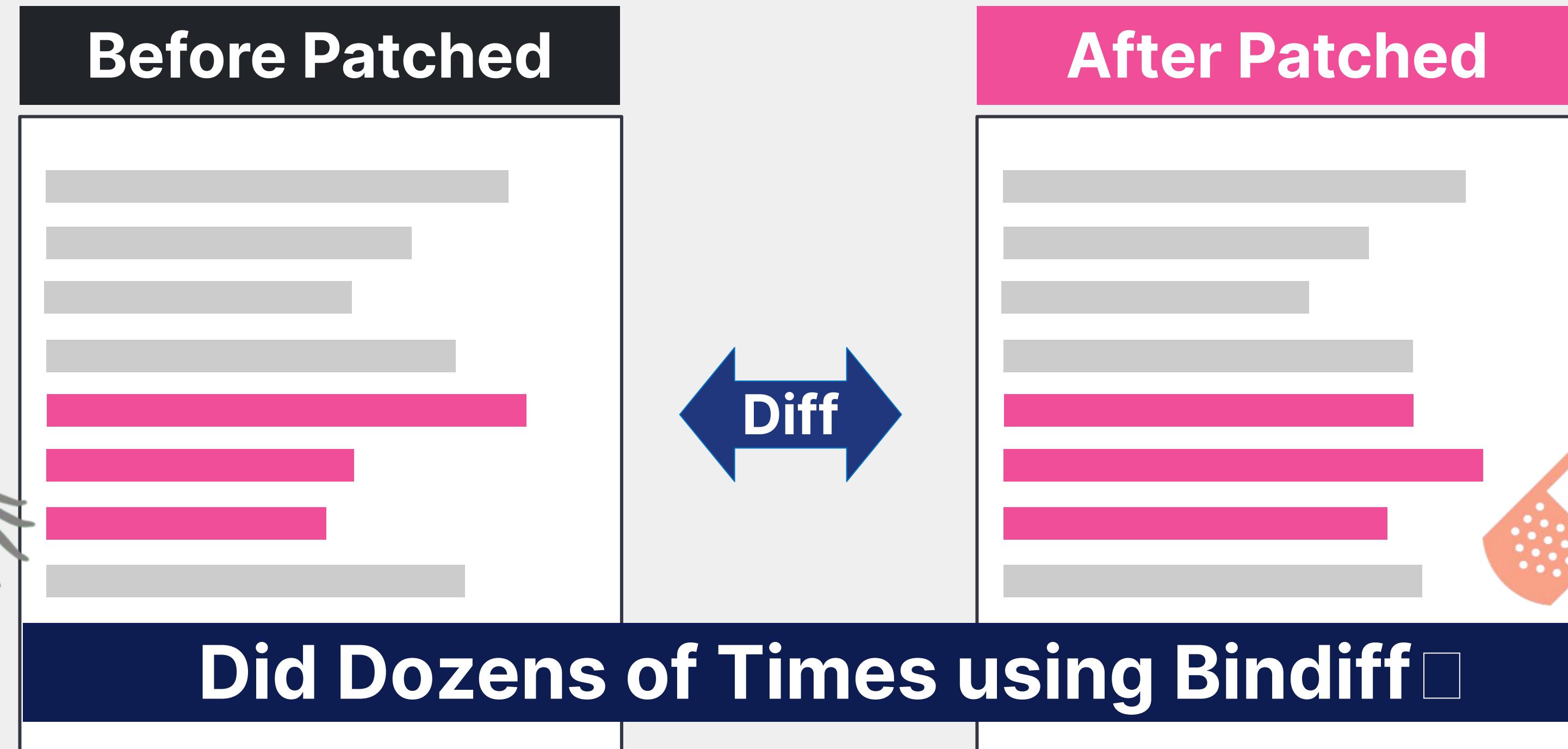
Diff

After Patched



Did Dozens of Times using Bindiff

Patch Diffing Manually to Find the Original Vuln Part

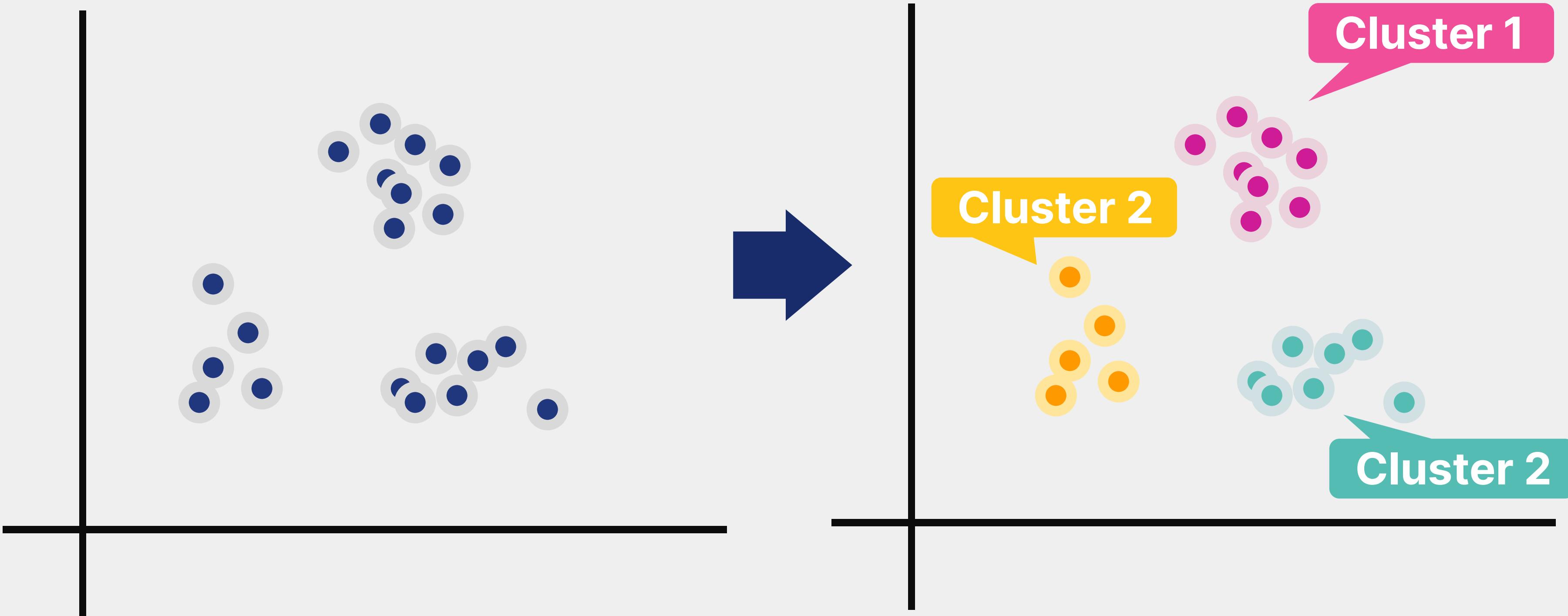


Can Patch Diffing be Facilitated by Using ML?

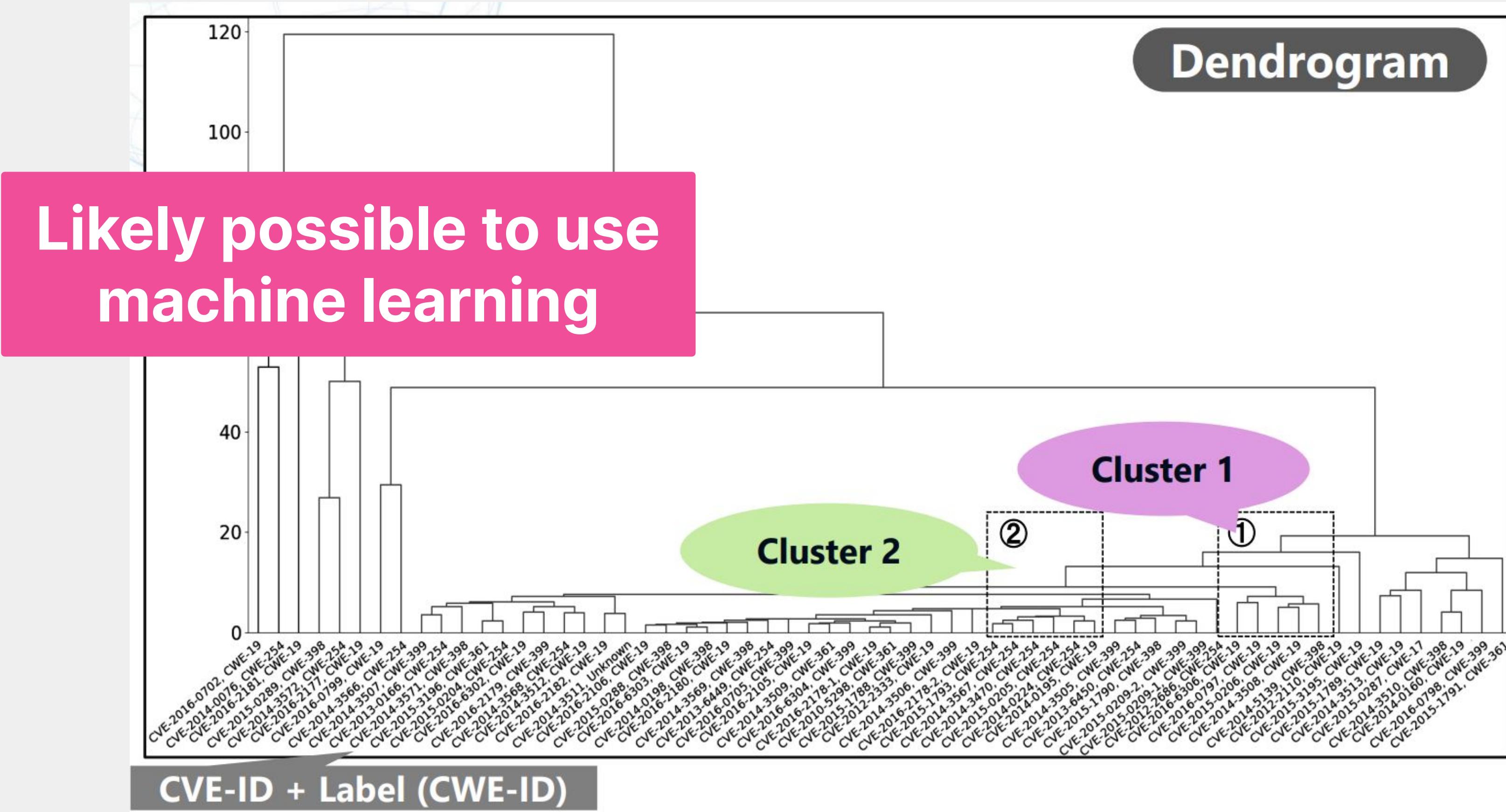
Clustering

Before Clustering

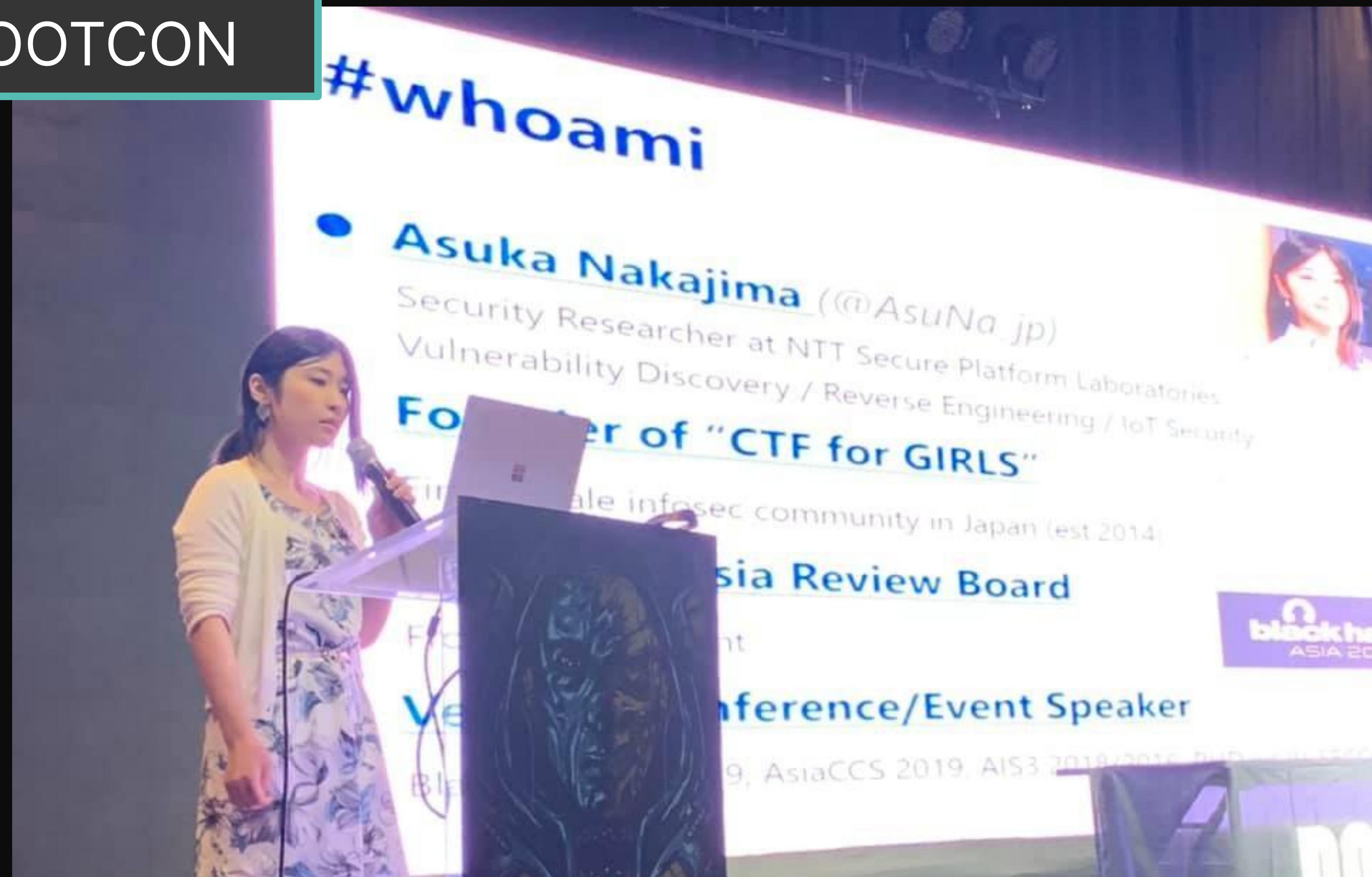
After Clustering



Found Patterns of Some Types of Vulnerability Fix



ROOTCON



1-Day Vulnerability Risk of IoT Devices

1-Day Vulnerability Risk of IoT Devices

CVE-2017-7852

Vendor

D-Link

Unsynchronized Patch Release

Model

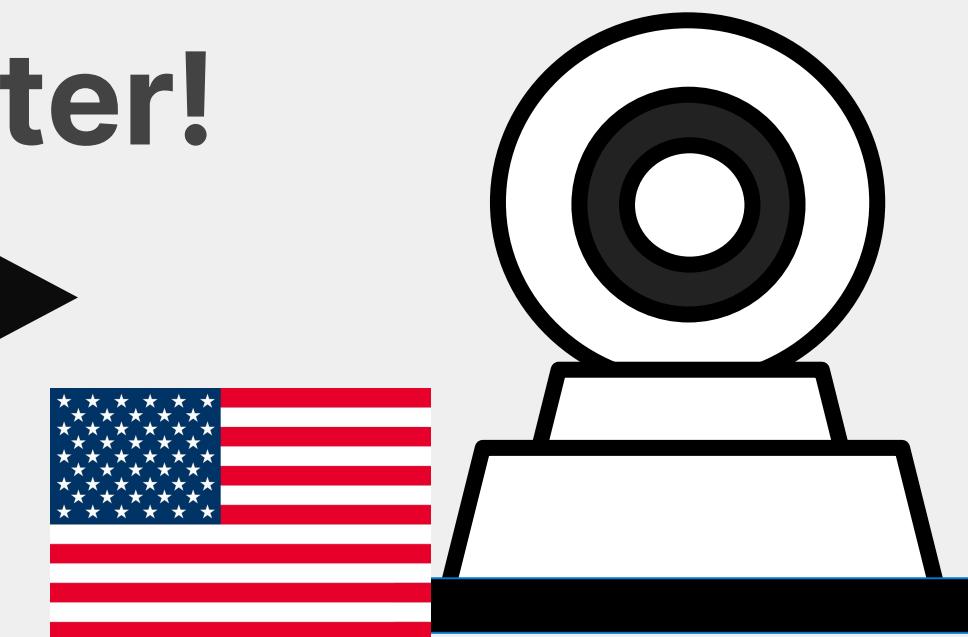
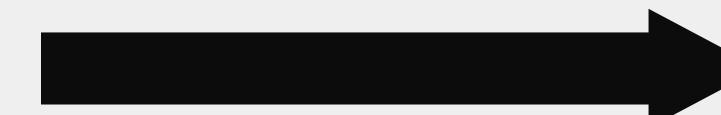
DCS-932L RevA



2015 Nov 18th

patch release

224 days later!



2016 Jul 19th

patch release

1-Day Vulnerability Risk of IoT Devices

CVE-2016-1556

Vendor

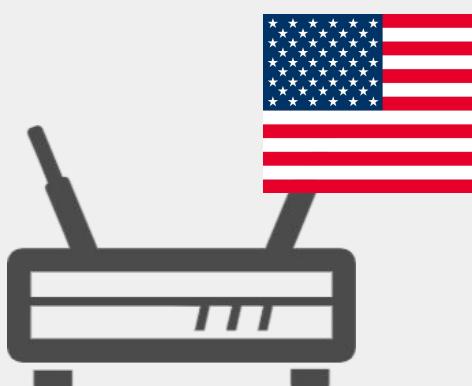
Netgear

Implicit End-of-Support (EoS)

Model

WN604

patch release



**Ver. 3.0.2
2012/Apr**

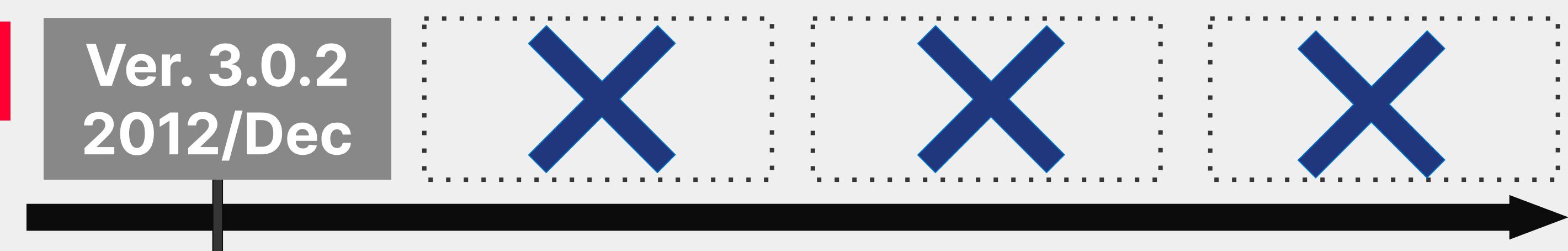
**Ver. 3.3.1
2015/May**

**Ver. 3.3.2
2015/Jul**

**Ver. 3.3.3
2016/Mar**



**Ver. 3.0.2
2012/Dec**



A Pilot Study on Consumer IoT Device Vulnerability Disclosure and Patch Release in Japan and the United States

Asuka Nakajima

NTT Secure Platform Laboratories
asuka.nakajima.db@hco.ntt.co.jp

Takuya Watanabe

NTT Secure Platform Laboratories
takuya.watanabe.yf@hco.ntt.co.jp

Eitaro Shioji

NTT Secure Platform Laboratories
eitaro.shioji.es@hco.ntt.co.jp

Mitsuaki Akiyama

NTT Secure Platform Laboratories
akiyama@ieee.org

Maverick Woo

Carnegie Mellon University
pooh@cmu.edu

ABSTRACT

With our ever increasing dependence on computers, many governments have started to investigate regulations on vulnerabilities and their lifecycle management. Although many previous works have studied this problem space for mainstream software packages and web applications, few studies have targeted consumer IoT devices. As a first step towards filling this void, this paper presents a pilot study on the vulnerability disclosures and patch release behaviors related to 3 prominent consumer IoT vendors in Japan and 3 in the United States. Our goals include (i) characterizing trends and risks using accurate data that spans a long period, and (ii) identifying problems, challenges, and potential approaches for future studies of this problem space. To this end, we collected all published vulnerabilities and their patches for the consumer IoT products by the included vendors between 2006 and 2017; then, we analyzed our

9–12, 2019, Auckland, New Zealand. ACM, New York, NY, USA, 8 pages.
<https://doi.org/10.1145/3321705.3329849>

1 INTRODUCTION

As our society continues to increase its reliance on computers large and small, vulnerabilities and their lifecycle management are gradually becoming a matter of public safety. In response, many governments have started to investigate regulating computer security through legislation/standards setting, e.g., [18, 22]. As we might expect, understanding the past and current practices of the stake-

**Joint Research with
Carnegie Mellon University**



#3

Each research took 1~3 years to complete 😱



Each research took 1~3 years to complete 😱

2000 hours & 100+meetings! □



Each research took 1~3 years to complete 😱

2000 hours & 100+meetings! ☐

Rejected many times 😢



Each research took 1~3 years to complete 😱

2000 hours & 100+meetings! ☐

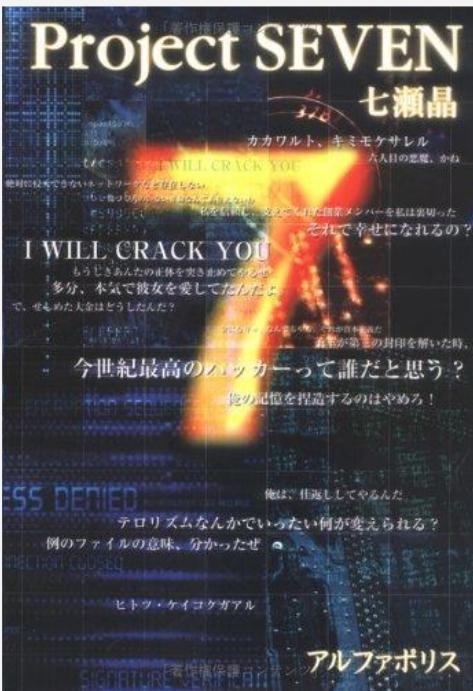
Rejected many times 😢

Some research has
not been published... 😞



Timeline

age 14



2004

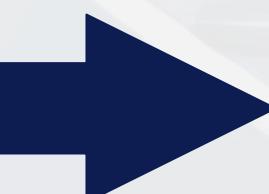
University
Days



Vuln
Research



2013



Timeline

age 14



2004

University
Days



2009

Vuln
Research



2013

Change
the world?



2019



Security Risk of OEM Supply Chain

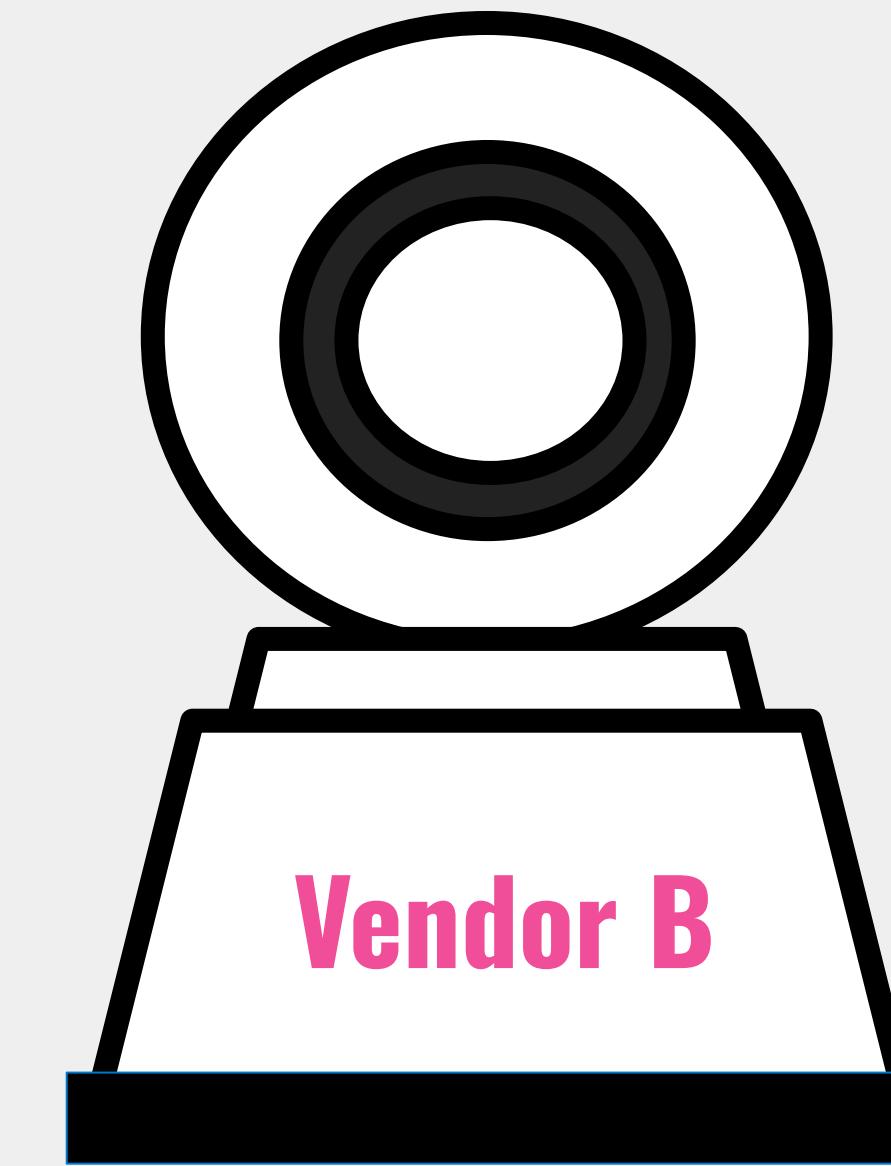
aka White Label Model

Security Risk of OEM Supply Chain

aka White Label Model



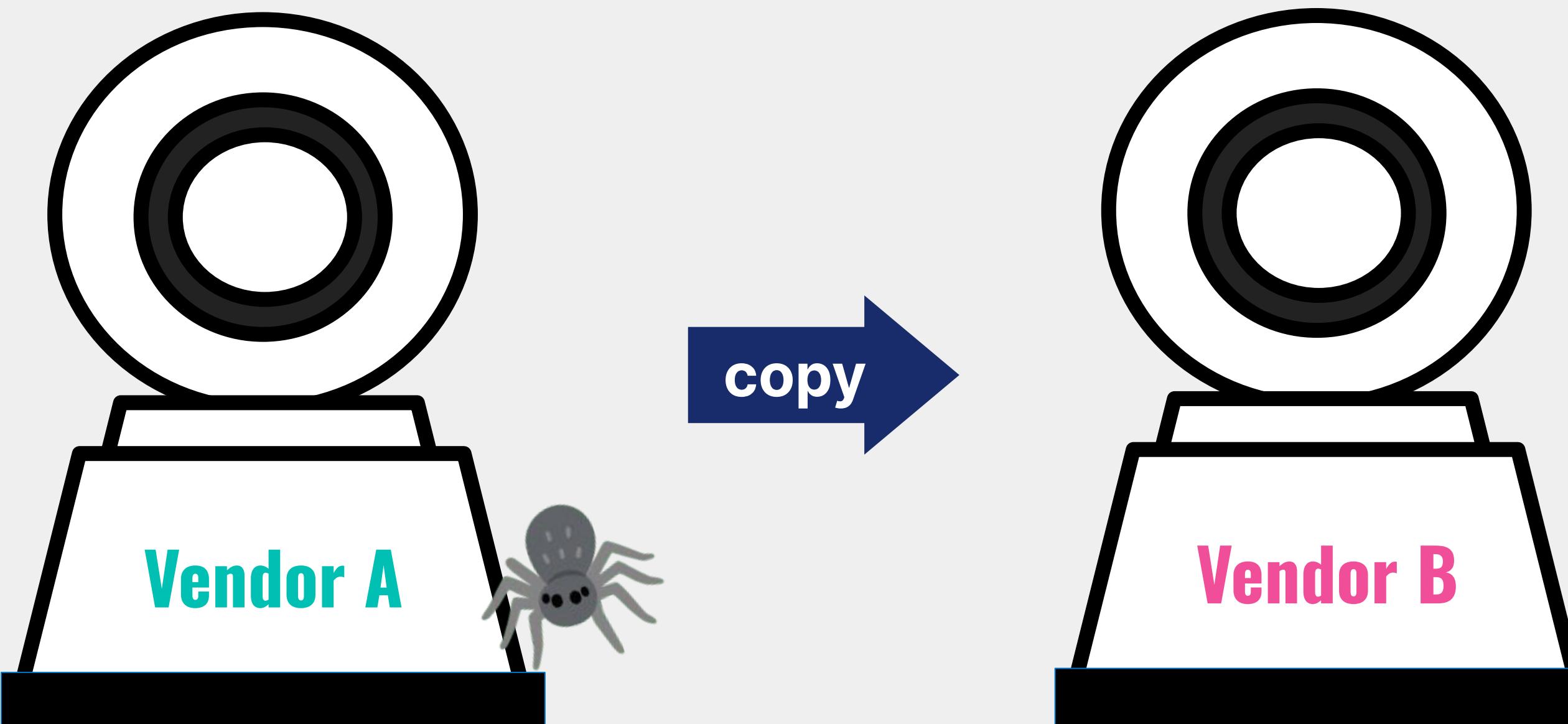
IoT Camera (Original)



IoT Camera (OEM)

Security Risk of OEM Supply Chain

aka White Label Model

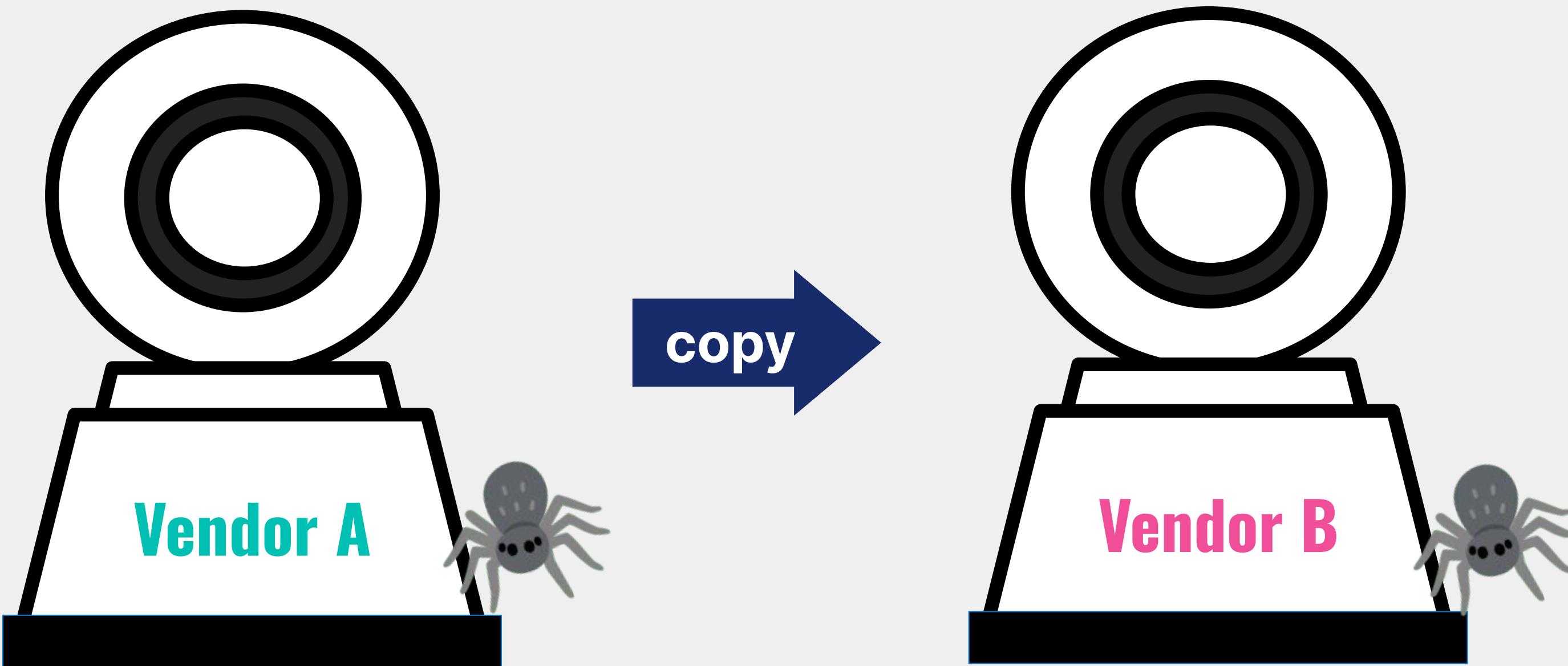


IoT Camera (Original)

IoT Camera (OEM)

Security Risk of OEM Supply Chain

aka White Label Model



IoT Camera (Original)

IoT Camera (OEM)

CVE-2010-4230



IoT Camera (Original)

Vendor

Camtron

Model

CMNC-200



IoT Camera (OEM)

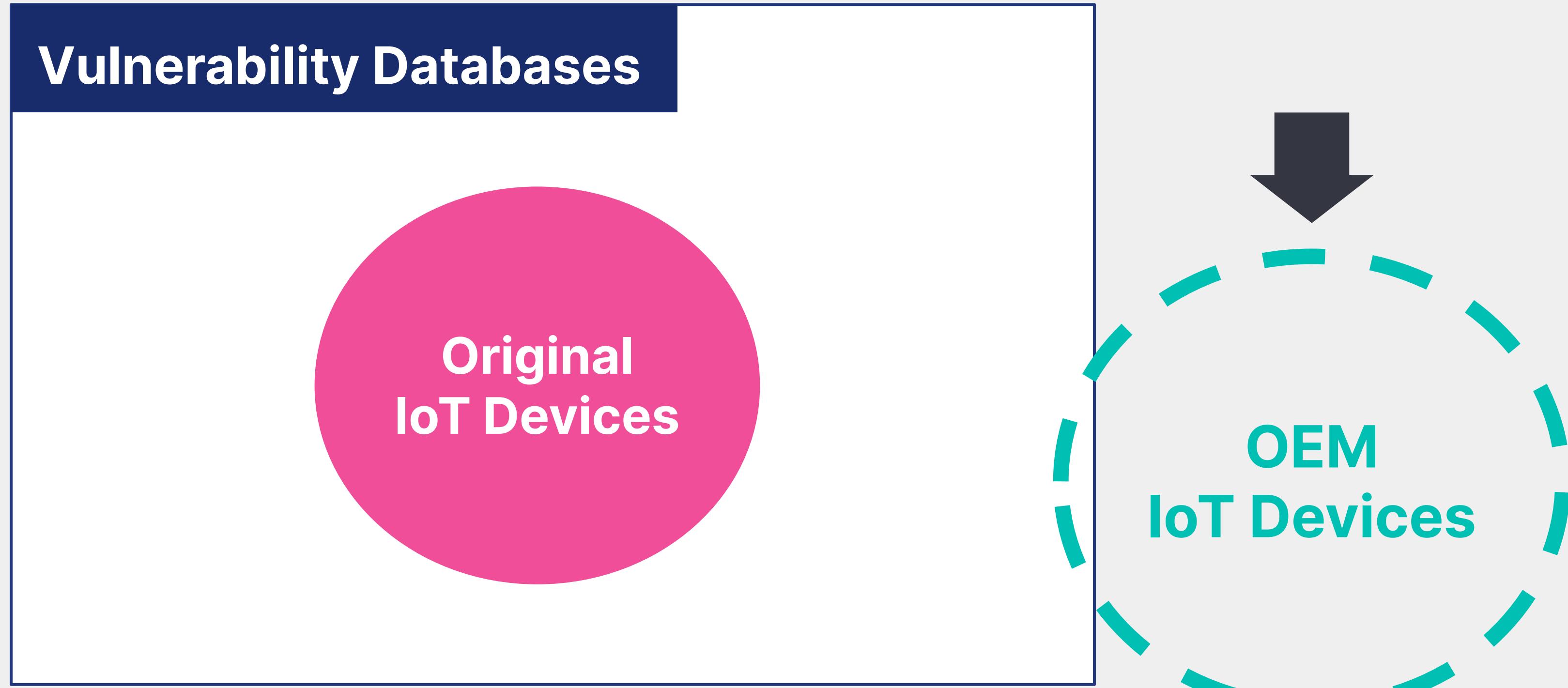
Vendor

Tecvoz

Model

CMNC-200

OEM Devices are NOT Included in Vuln DBs



OEM Device users cannot know about the risks

Created an OEM IoT Device Search Engine

OEM Finder

Search and Find Vulnerable OEM IoT Devices!

select file...

Show Advanced Search Option

Search OEM Device Search Original Device

About OEM Finder

OEM Finder is a search engine that helps you to find vulnerable OEM IoT devices based on the similarity of its appearance between the OEM and original device. By uploading a photo of vulnerable IoT devices, this web service can list the OEM device candidates that potentially contain the identical vulnerability.

[Learn More](#)

Contact

This is a project by Asuka Nakajima. Feel free to get in touch if you have any questions or suggestions.

※ This demo website is currently closed

Search Result



[View Detail](#)

MPT Electrical Products



SL 300WADT ITW



[View Detail](#)

Kulay



SYNCHROSADE-ELECTRICALS



[View Detail](#)

PN-CA



Unknown



[View Detail](#)

TRINITY-ELECTRONICS



Unknown



[View Detail](#)

TEDDY



TD-300



[View Detail](#)

STD-C



STD-C



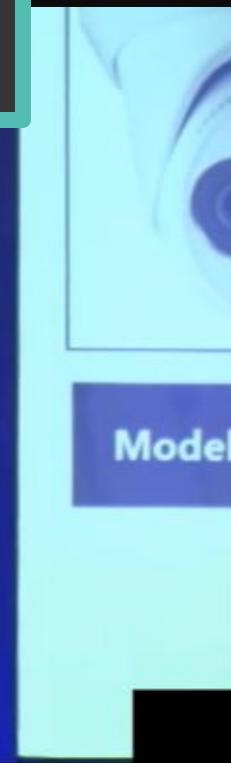
[View Detail](#)

STD-C



STD-C

BlackHat Europe



Case Study 1: Hikvision

black hat
EUROPE 2019

black hat®
EUROPE 2019

DECEMBER 2-5, 2019

EXCEL LONDON, UK

CVE-2017-7921 & CVE-2017-7923

OEM Device Candidates

| Original | Vendor: KT & C Model: KNC-P3TR6XIR | Vendor: PNET Model: PN-402EX | Vendor: PWS Security Model: Unknonwn | Vendor: LTS Model: CMIP3032-28 | Vendor: Orange Sources Model: Unknown |
|---------------------|--|----------------------------------|---|-----------------------------------|---|
| | | | | | |
| Model: ds-2cd2312-i | Vendor: P2P Security Model: Unknown | Vendor: HDView Model: Unknown | Vendor: AVUE Model: AV50HTWX | Vendor: CMPLE Model: 1287-N | Vendor: Securitiy Camera King Model: IPOD-PR2EXIRE28 |

Suchmaschine entdeckt Sicherheitslücken in Security-Kameras

Von Kristian Kijßling - 05. Dezember 2019

Auf der Black Hat Europe 2019 haben japanische Security-Forscher von NTT eine Online-Suche vorgestellt, mit der sie Sicherheitslücken in No-Name-Security-Kameras leichter entdecken können.

Wer heute eine Netzwerk-basierte Sicherheitskamera kauft, erhält oft unter verschiedenen Namen das gleiche Gerät. Das ist so, weil ein OEM-Hersteller seine Kamera an verschiedene OEM-Anbieter verkauft, die dann ihre Sticker auf das Gerät pappen und es in den Handel bringen. Das aber bringt in puncto Sicherheit gleich mehrere Probleme mit sich.

Oft stecken in der ausgelieferten Firmware des Originalanbieters Sicherheitslücken. Stopft der OEM-Hersteller diese Sicherheitslücken, landen diese Fixes dennoch häufig nicht in den verkauften Geräten der OEM-Anbieter. Zugleich verraten die [National Vulnerability Database](#) (NVD) und die Datenbank der [Common Vulnerabilities and Exposures](#) (CVE) nicht, in welchen Geräten welcher weiteren Anbieter diese Sicherheitslücken stecken.

Zudem sind auch die OEM-Anbieter nicht wirklich daran interessiert, dass die Kunden erfahren, von dem die Kamera eigentlich stammt. Der OEM-Hersteller ist daher oft nicht offensichtlich. Kaufen Admins solche No-Name-Security-Kameras, müssen sie also selbst herausfinden, wie sicher diese sind. Sie können dazu die Firmware dumpen, den OEM-Hersteller finden und die Firmwaredateien verschiedener Modelle vergleichen.

**[https://www.linux-magazin.de/news/suchmaschine-entdeckt-sic
herheitsluecken-in-security-kameras/](https://www.linux-magazin.de/news/suchmaschine-entdeckt-sicherheitsluecken-in-security-kameras/)**

Finen anderen Weß schlägt die Japanerin Asuka Nakaiima vor, die bei NTT als Security-Forscher arbeitet. Sie und ihr

Suchmaschine entdeckt Sicherheitslücken in Security-Kameras

Von Kristian Kjellberg - 05. Dezember 2019

Auf der Black Hat Europe 2019 haben japanische Security-Forscher von NTT eine Online-Suche vorgestellt, die sie Sicherheitslücken in No-Name-Security-Kameras leichter entdecken können.

Wer heute eine Netzwerk-basierte Sicherheitskamera kauft, erhält oft unter verschiedenen Namen das gleiche Gerät.

Das ist so, weil ein OEM-Hersteller seine Kamera an verschiedene OEM-Anbieter verkauft, die dann ihre Sticker auf das Gerät pappen und es in den Handel bringen. Das aber bringt in puncto Sicherheit gleich mehrere Probleme mit sich.

Oft stecken in der ausgelieferten Firmware des Originalanbieters Sicherheitslücken. Stopft der OEM-Hersteller diese Sicherheitslücken, landen diese Fixes dennoch häufig nicht in den verkauften Geräten der OEM-Anbieter. Zugleich verraten die National Vulnerability Database (NVD) und die Datenbank der Common Vulnerabilities and Exposures (CVE) nicht, in welchen Geräten welcher weiteren Anbieter diese Sicherheitslücken stecken.

Zudem sind auch die OEM-Anbieter nicht wirklich daran interessiert, dass die Kunden erfahren, von dem die Kamera eigentlich stammt. Der OEM-Hersteller ist daher oft nicht offensichtlich. Kaufen Admins solche No-Name-Security-Kameras, müssen sie also selbst herausfinden, wie sicher diese sind. Sie können dazu die Firmware dumpen, den OEM-Hersteller finden und die Firmware-Versionen der Modelle vergleichen.

<https://www.linux-magazin.de/news/suchmaschine-entdeckt-sicherheitsluecken-in-security-kameras/>

Finen anderen We& schlägt die Japanerin Asuka Nakaiima vor, die bei NTT als Security-Forscher arbeitet. Sie und ihr



Black Hat Asia

May 10-13, 2022

Hybrid/Marina Bay Sands, Singapore

Black Hat USA

August 6-11, 2022

Las Vegas, NV, U

Black Hat Europe Brings A Bevy of IoT Security Insights



Black Hat Staff
Event Updates

Attend this London event next month for the latest on how security researchers are finding (and solving) security vulnerabilities in all of your favorite Internet-connected devices.

As the year winds down around us, people around the world are spending more time at home, visiting friends and family. Many of those homes are filled

<https://www.darkreading.com/black-hat/black-hat-europe-brings-a-bevy-of-iot-security-insights/d/d-id/1336382>

learn about the latest IoT security tricks and techniques.

Suchmaschine entdeckt Sicherheitslücken in Security-Kameras

Von Kristian Kjæling - 05. Dezember 2019

Auf der Black Hat Europe 2019 haben japanische Security-Forscher von NTT eine Online-Suche vorgestellt, die sie Sicherheitslücken in No-Name-Security-Kameras leichter entdecken können.

Wer heute eine Netzwerk-basierte Sicherheitskamera kauft, erhält oft unter verschiedenen Namen das gleiche Gerät. Das ist so, weil ein OEM-Hersteller seine Kamera an verschiedene OEM-Anbieter verkauft, die dann ihre Software pappen und es in den Handel bringen. Das aber bringt in puncto Sicherheit gleich mehrere Probleme mit sich.

Oft stecken in der ausgelieferten Firmware des Originalanbieters Sicherheitslücken. Stopft der OEM-Hersteller diese Fixes, landen diese Fixes dennoch häufig nicht in den verkauften Geräten der OEM-Anbieter. Das verraten die National Vulnerability Database (NVD) und die Datenbank der Common Vulnerabilities and Exposures (CVE) nicht, in welchen Geräten welcher weiteren Anbieter diese Sicherheitslücken stecken.

Zudem sind auch die OEM-Anbieter nicht wirklich daran interessiert, dass die Kunden erfahren, von dem Hersteller stammt. Der OEM-Hersteller ist daher oft nicht offensichtlich. Kaufen Admins solche No-Name-Kameras, müssen sie also selbst herausfinden, wie sicher diese sind. Sie können dazu die Firmware dumpen und sie mit anderen Firmwares derselben Modelle vergleichen.

<https://www.linux-magazin.de/news/suchmaschine-entdeckt-sicherheitsluecken-in-security-kameras/>

Finen anderen Weß schlägt die Japanerin Asuka Nakaiima vor, die bei NTT als Security-Forscher arbeitet. Sie



Black Hat Asia
May 10-13, 2022
Hybrid/Marina Bay Sands, Singapore

Black Hat USA
August 6-11, 2022
Las Vegas, NV, U

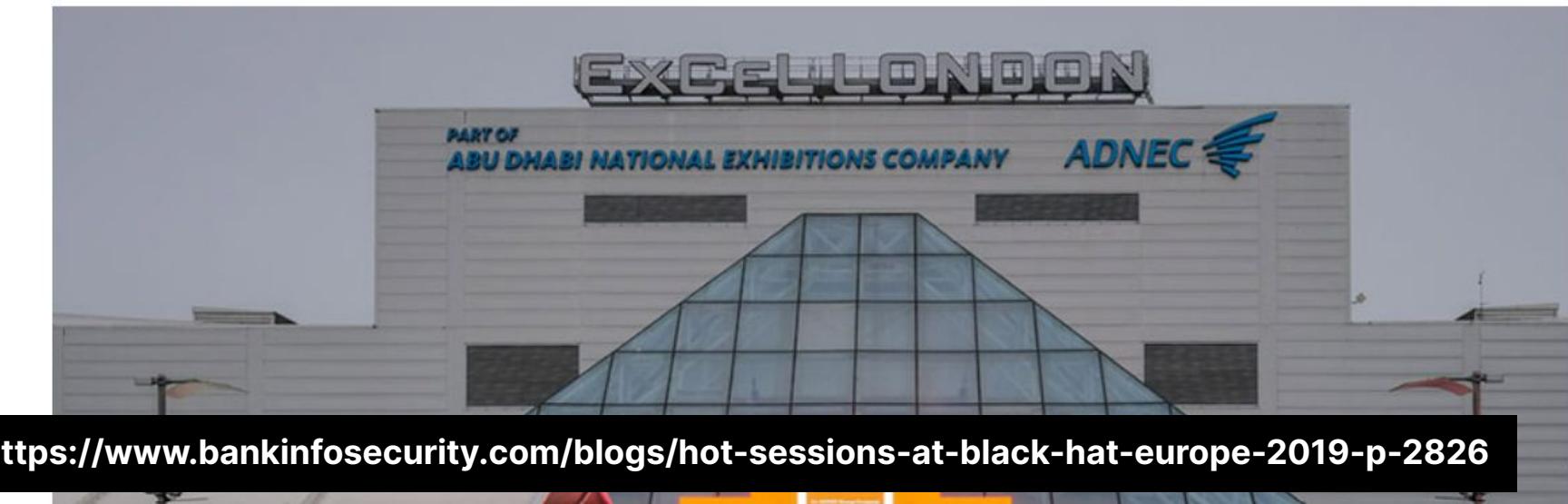
Black Hat Europe Brings A Bevy of IoT Security Insights

Attend this London event next month for the latest on how security

15 Hot Sessions at Black Hat Europe 2019

Contactless Payments, IoT, False Flag Attacks and More in the Spotlight

Mathew J. Schwartz (@euroinfosec) • December 3, 2019

[Share](#)[Tweet](#)[Share](#)[Get Permission](#)

<https://www.bankinfosecurity.com/blogs/hot-sessions-at-black-hat-europe-2019-p-2826>



Embedded Linu

Administration

Startseite > New

Suchmasc

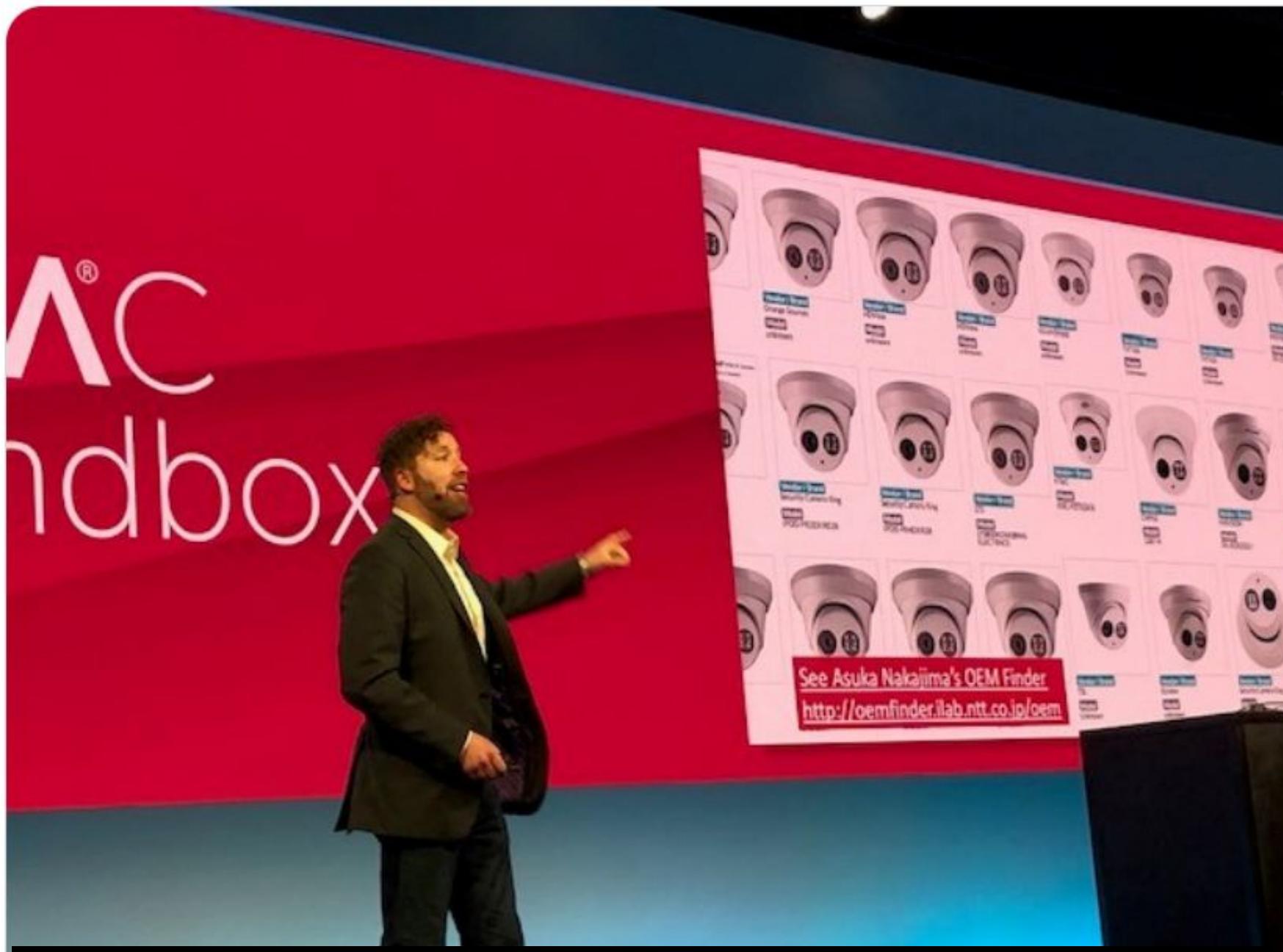
Von Kristian Kjellin

Auf der Black H
der sie SicherheWer heute eine N
Das ist so, weil e
Gerät pappen urOft stecken in de
Sicherheitslücke
verraten die Nat
(CVE) nicht, in weZudem sind auch
eigentlich stamm
Kameras, müsse
OEM-Hersteller<https://www.linuxmagazin.de/herheitsluecken-in-embedded-systemen/>

Finen anderen W

<https://www.bankinfosecurity.com/blogs/hot-sessions-at-black-hat-europe-2019-p-2826>

午前3:00 · 2020年3月4日



ead

SIGN UP FOR OUR
NEWSLETTERS

Video Tech Library University Security Now Calendar Black Hat News On

TACKS /
EACHES APP SEC CLOUD ENDPOINT IoT OPERATIONS PERIMET

Black Hat Asia

May 10-13, 2022

Hybrid/Marina Bay Sands, Singapore

Black Hat USA

August 6-11, 202

Las Vegas, NV, U

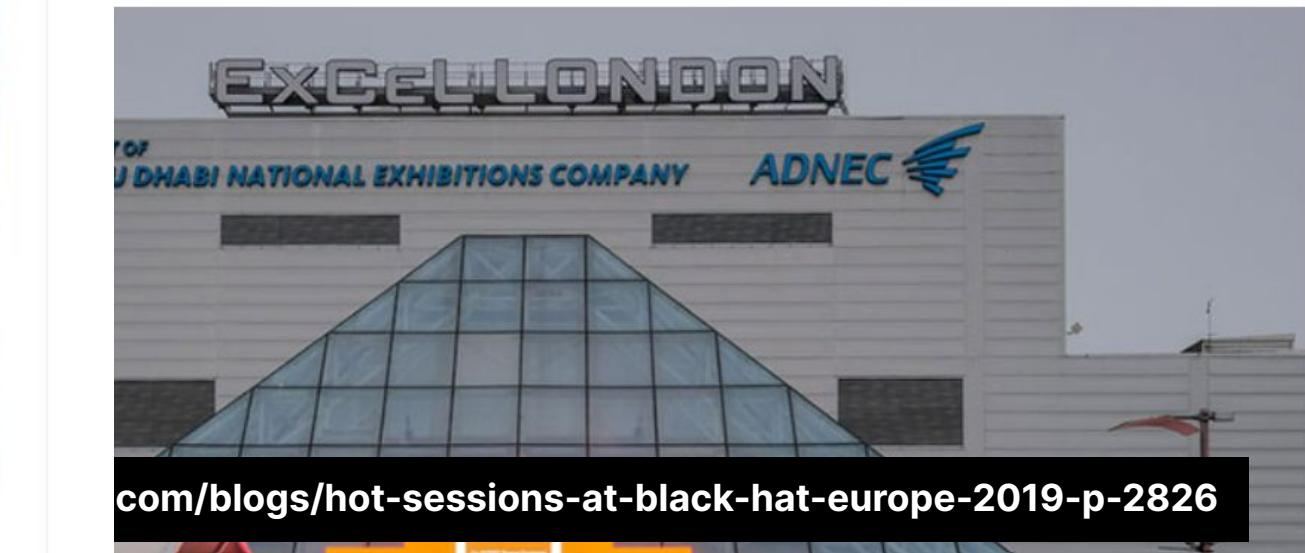
Black Hat Europe Brings A Bevy of Security Insights

this London event next month for the latest on how security

ons at Black Hat Europe 2019

else Flag Attacks and More in the Spotlight

December 3, 2019

[Tweet](#) [Share](#)[Get Permission](#)

Auf der Black H
der sie Sicherhe

Wer heute eine
Das ist so, weil e
Gerät pappen un

Oft stecken in den Sicherheitslücken verraten die Natur (CVE) nicht, in wen

Zudem sind auch eigentlich stamm Kameras, müsse

<https://www.linux-herheitsluecken.info>

Finen anderen W

<https://>

“See Asuka Nakajima’s OEM Finder”

午前3:00・2020年3月4日

Last week was a big week for **#SBOM**. N
#BSidesSF2020, **#CyberTalks**, and @R:
the talk he gave at RSA here: [rsaconfere](#)

ポストを翻訳



United State's National Telecommunications and Information Administration

May 10-13, 2022

Hybrid/Marina Bay Sands, Singapore

August 6-11, 202

Las Vegas, NV, U

ck Hat Europe Brings A Bevy of Security Insights

this London event next month for the latest on how security

dns at Black Hat Europe 2019

False Flag Attacks and More in the Spotlight

December 3, 20



[Get Permission](#)





Last week was a big week for **#SBOM**. N
#BSidesSF2020, **#CyberTalks**, and @RS
the talk he gave at RSA here: [rsaconfere](#)

ポストを翻訳

United State's National Telecommunications and Information Administration

May 10-13, 2022

Hybrid/Marina Bay Sands, Singapore

August 6-11, 202

Las Vegas, NV, U

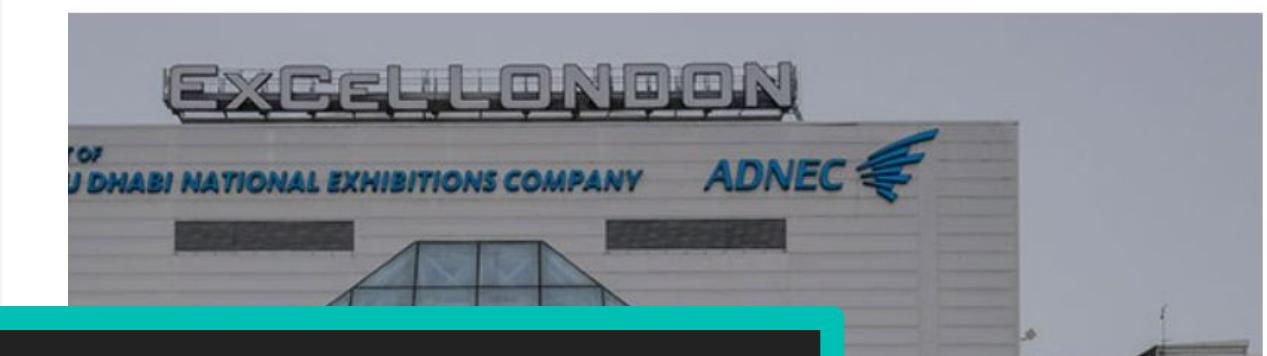
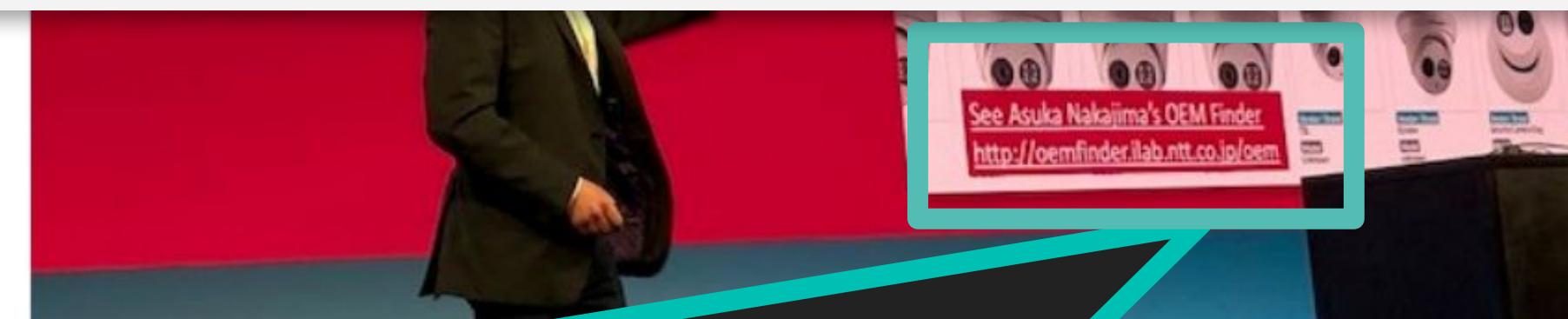
SBOM (Software Bill of Materials)

<https://www.ntia.gov/page/software-bill-materials>

Zudem sind auch
eigentlich stamm
Kameras, müsse
OEM-Hersteller

<https://www.linuxherheitsluecken.info>

Finen anderen W



“See Asuka Nakajima’s OEM Finder”

<https://>

ope-2019-p-2826

Presented at One of the Top Tier
Hacker Conferences, and Made a
Positive Impact to the World! 

Dream has come true?

Timeline

age 14



2004

University
Days



2009

Vuln
Research



2013

Change
the world?



2019



Rethinking My Career

Although I was able to **make a positive impact on the world** 

through my research, **none of them have been utilized for business or released as tools** 

Rethinking My Career

Want/Need More **Defence & Developer Side Experience** to

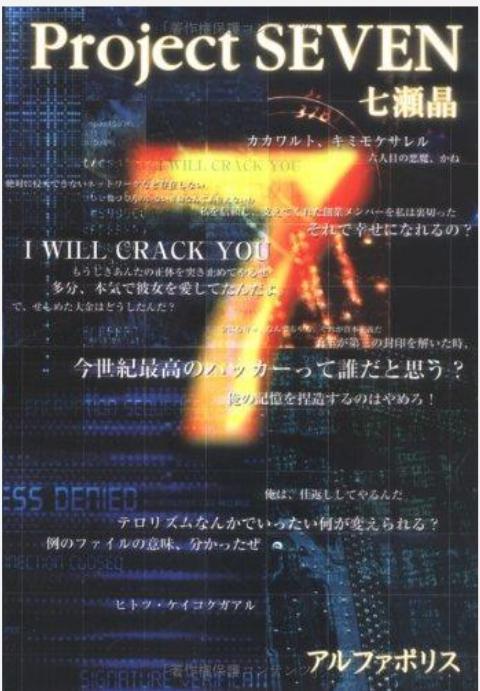
Continue Making Positive and

Sustainable Impact on the World



Timeline

age 14



2004

University
Days



2009

Vuln
Research



2013

Change
the world?



2019

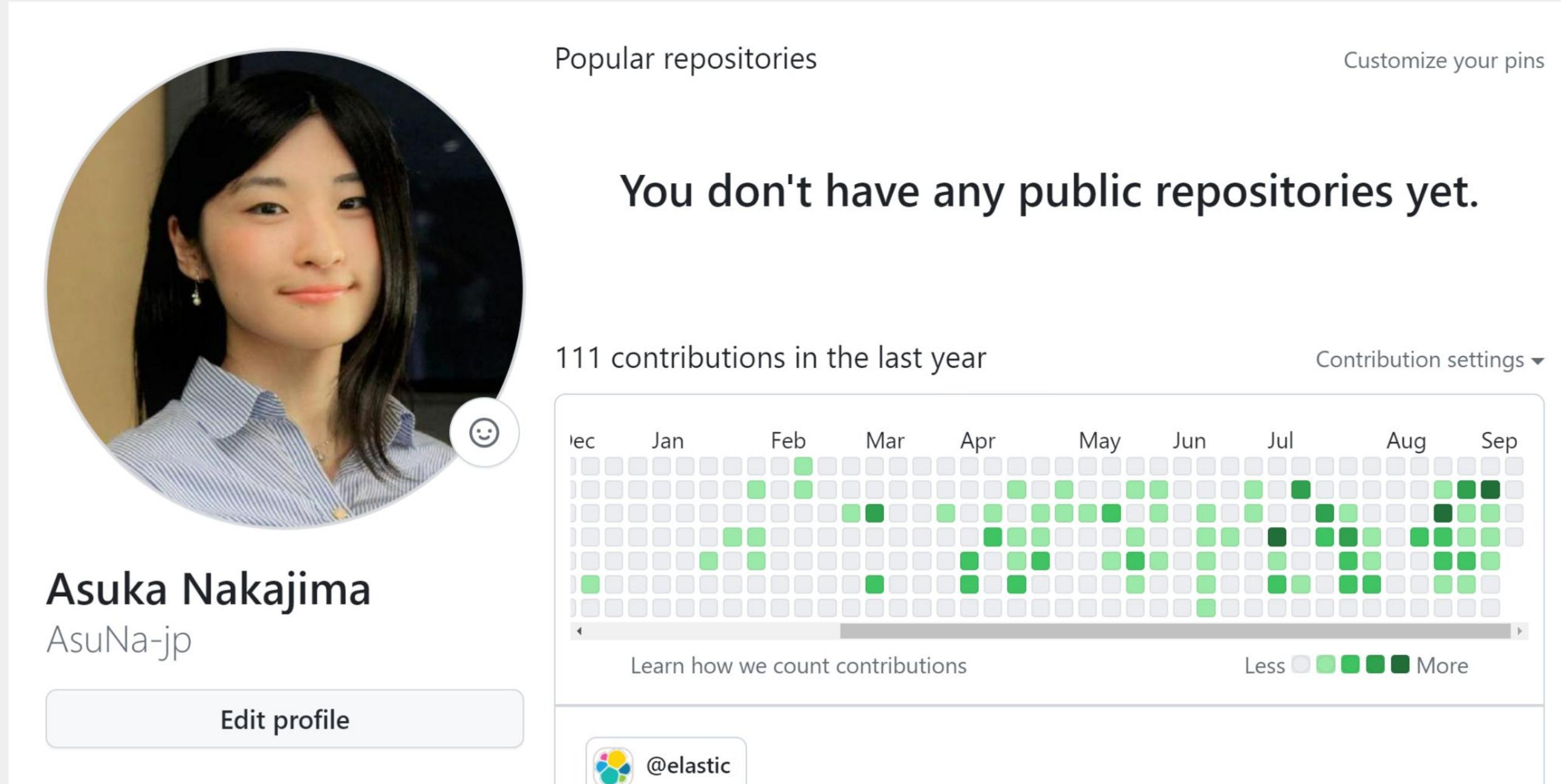
Defence
side!



2022

Endpoint Security R&D (EDR)

EDR: Endpoint Detection and Response



A GitHub profile screenshot for user 'Asuka Nakajima' (AsuNa-jp). The profile picture is a circular photo of a young woman with long dark hair. To the right of the photo are two buttons: 'Popular repositories' and 'Customize your pins'. Below the photo, the name 'Asuka Nakajima' and handle 'AsuNa-jp' are displayed. A large button labeled 'Edit profile' is at the bottom left. The main content area shows a message: 'You don't have any public repositories yet.' Above this message is a statistic: '111 contributions in the last year'. Below the statistic is a heatmap showing contribution counts by month from Dec to Sep. The heatmap uses a color scale from light gray ('Less') to dark green ('More'). At the bottom of the heatmap, there are links to 'Learn how we count contributions' and a legend for the color scale. The @elastic icon is at the bottom right of the profile area.



Elastic Defend

Involved in new feature development which uses Windows ETW



My Journey Continues..



First Female Infosec Community in Japan



- ✓ Established in **2014**
- ✓ Supported by **SECCON**
- ✓ Started from about **10** members (now about 50)
- ✓ Hold **Women-Only CTF Workshops & CTFs**



First Workshop was held in June 2014 (Tokyo)



More than **70** people participated in our workshop

Received many **positive feedbacks** from attendees

CTF Workshop (22 times) / CTF (5 times)

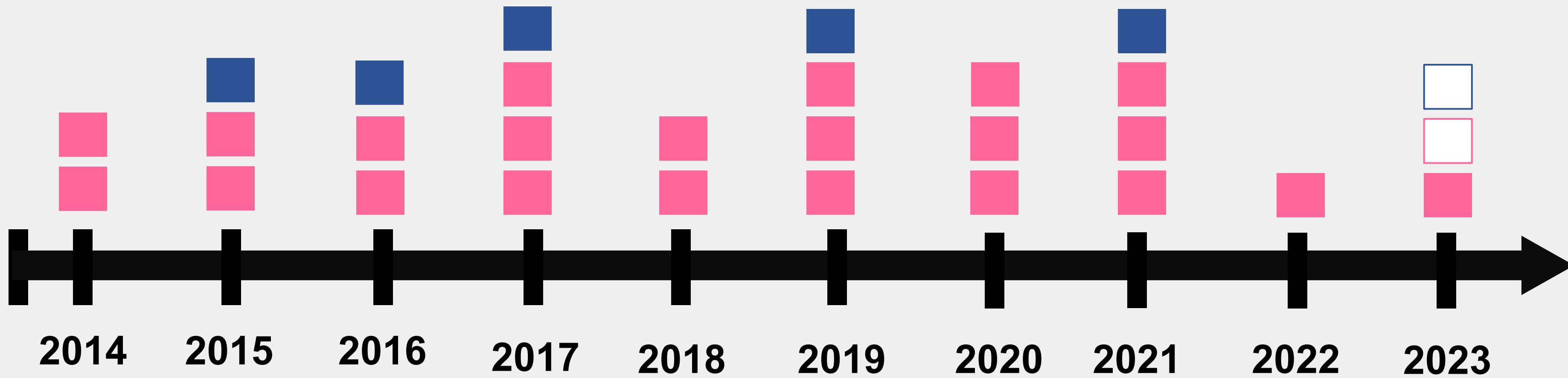
More than **1200** women have participated in our workshops



CTF Workshop
CTF

COVID19

Online Workshops



Photos





HITCON GIRLS
@hitcongirls

We have finished the talk in BlackHat 2019 USA: "Communities for Women". If any of you are interested in our work, please contact us!

#BHUSA

Asuka Nakajima | #CTFforGIRLS @ctf4g

Suhee Kang | #PowerofXX @POC_Crew

Hazel Yen | #HITCONGIRLS @hitcongirls

ツイートを翻訳



black hat USA 2019

Women in Security

Building a Female InfoSec Community in Korea, Japan, and Taiwan

Suhee Kang, Asuka Nakajima, Hazel Yen

About Today's Talk

Introduce Three Representative Asian Female Communities
Power of XX (Korea), CTF for GIRLS (Japan), HITCON GIRLS (Taiwan)

South

Founder of Power of XX Est. 2011 Suhee Kang

Founder of CTF for GIRLS Est. 2014.06 Asuka Nakajima

Co-Founder of HITCON GIRLS Est. 2014.12 Hazel Yen

What we will talk

- How We Build & Maintain the Community
- What We Have Achieved
- How We Tackled Various Challenges

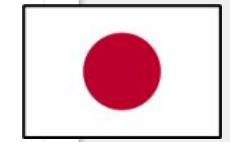
BlackHat USA 2019

Women in Security: Building a Female InfoSec Community in Korea, Japan, and Taiwan



Power of XX

- Suhee kang (South Korea)



CTF for GIRLS

- Asuka Nakajima (Japan)



HITCON GIRLS

- Hazel Yen (Taiwan)

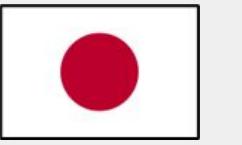
SECCON 2020

Winja × CTF for GIRLS Panel Discussion



Winja

- Riddhi Shree (India)



CTF for GIRLS

- Asuka Nakajima (Japan)

Winja Meets CTF for GIRLS (CTF4G) | SECCON 2020

Saturday, Dec 19, 2020 winja ctf4g seccon 2020

Representatives of Winja CTF (India) and CTF for GIRLS (Japan) communities had a conversation during SECCON 2020 con

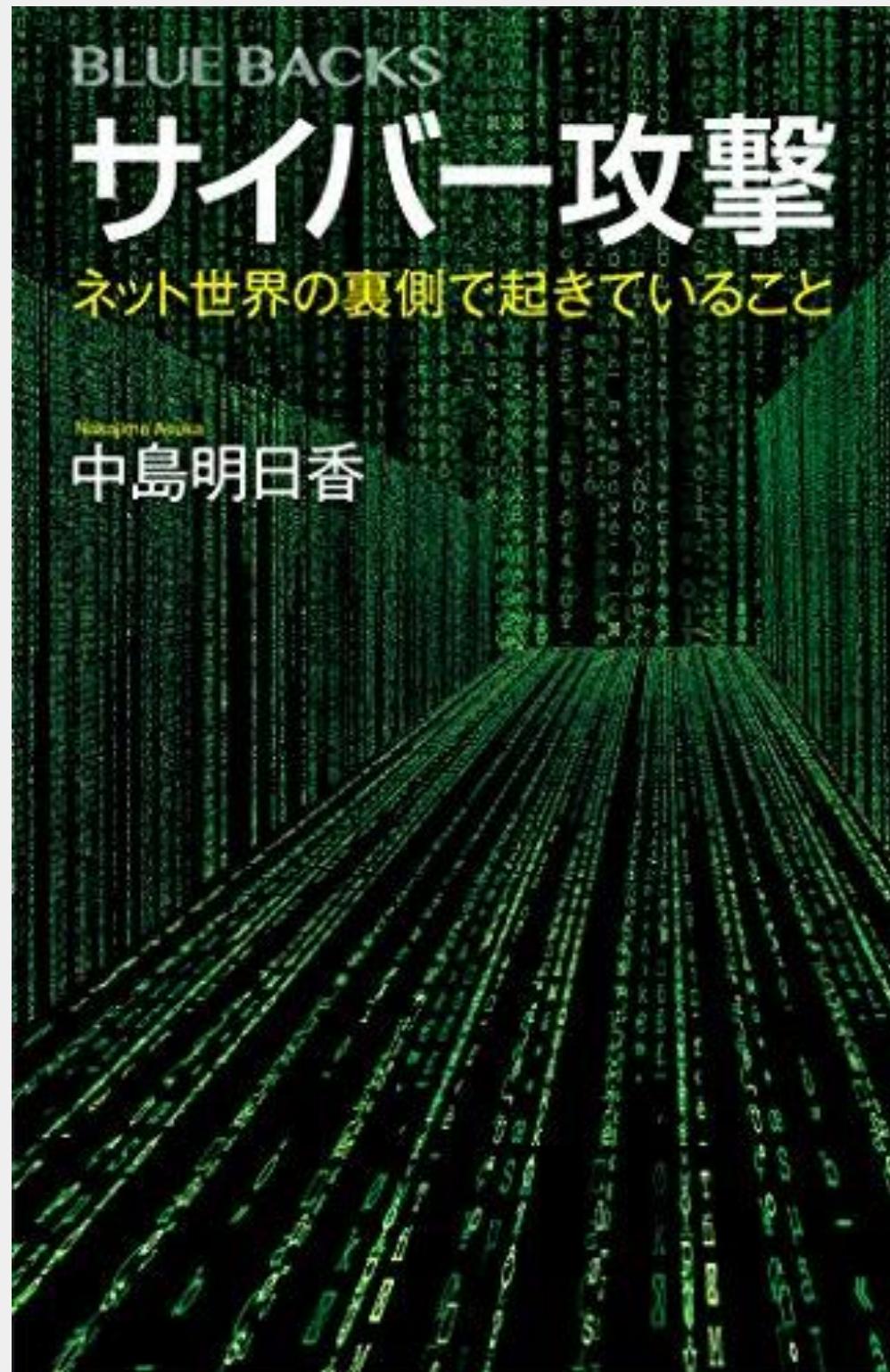
Watch the complete conversation that happened during [SECCON 2020](#) on [SECCON YouTube channel](#):



**CTF for GIRLS also provided a
CTF challenge for Winja CTF 2021!**



Raising Security Awareness



Published a book  called
“**Cyber Attack**” which talk
about software vulnerabilities
to the general public

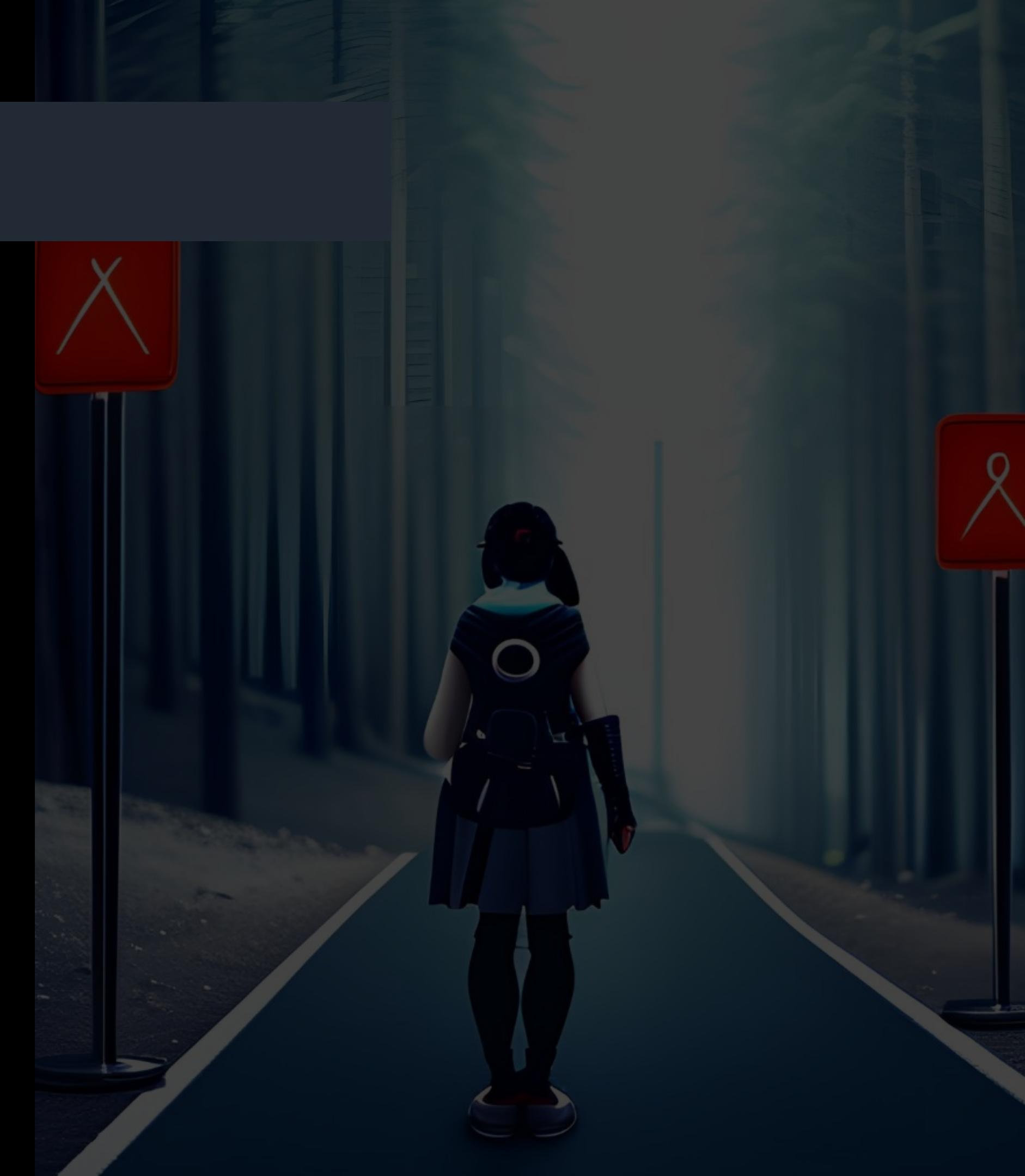
Sold about 20000 Copies! 😊

Takeaways

#1

#2

#3



Takeaways

#1

Importance of Mastering the Basics

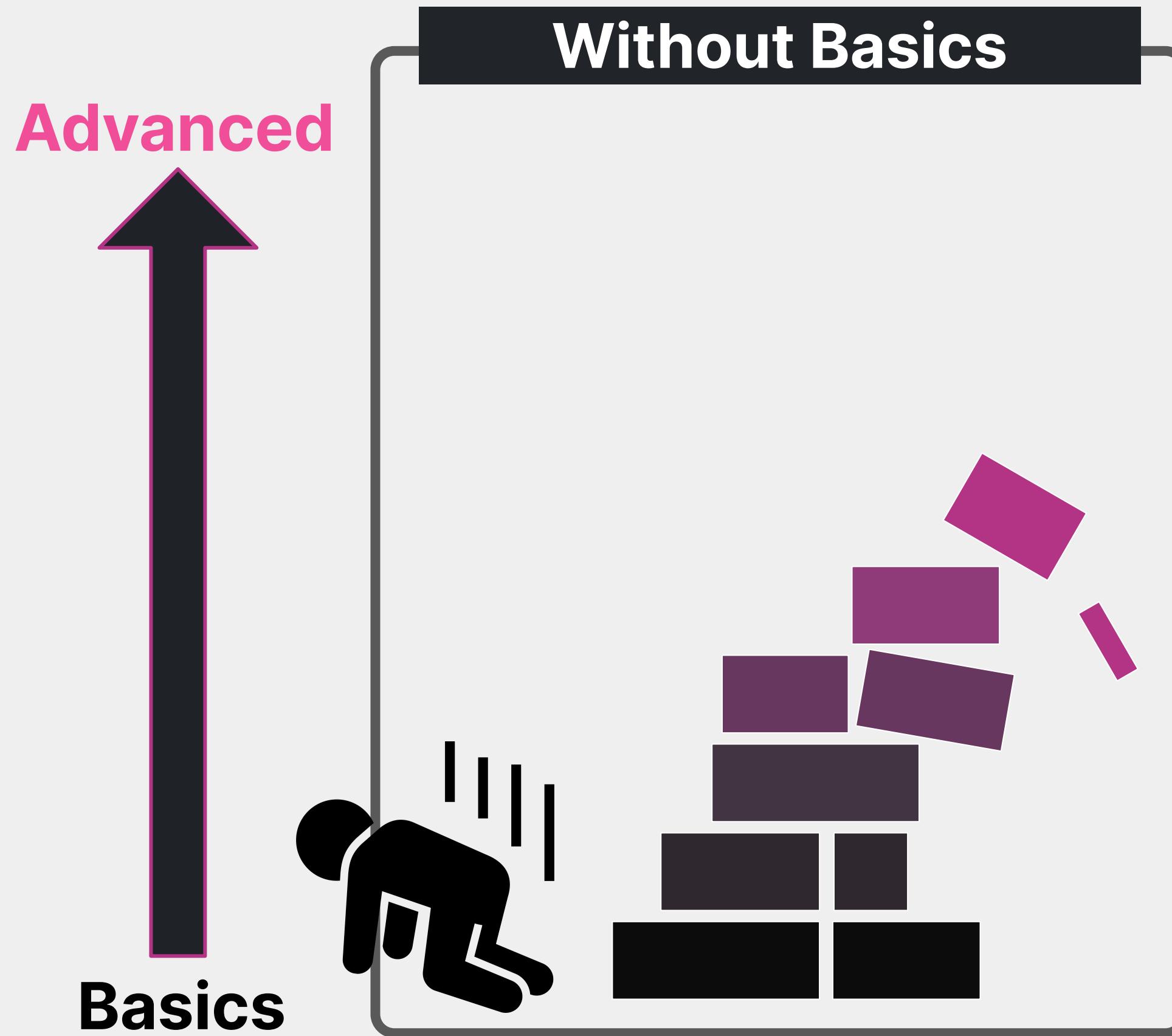
#2

#3



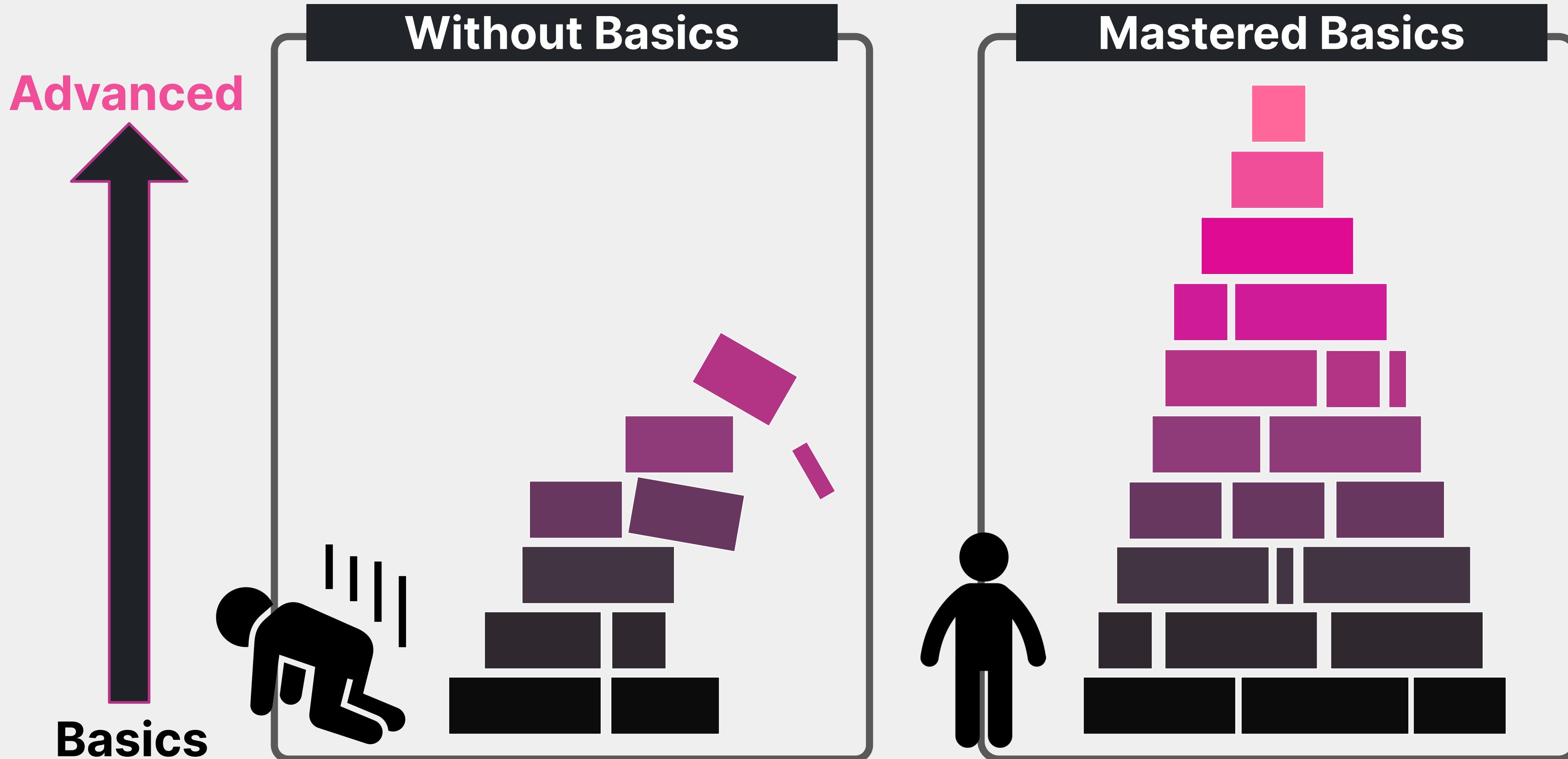
#1

Importance of Mastering the Basics



#1

Importance of Mastering the Basics



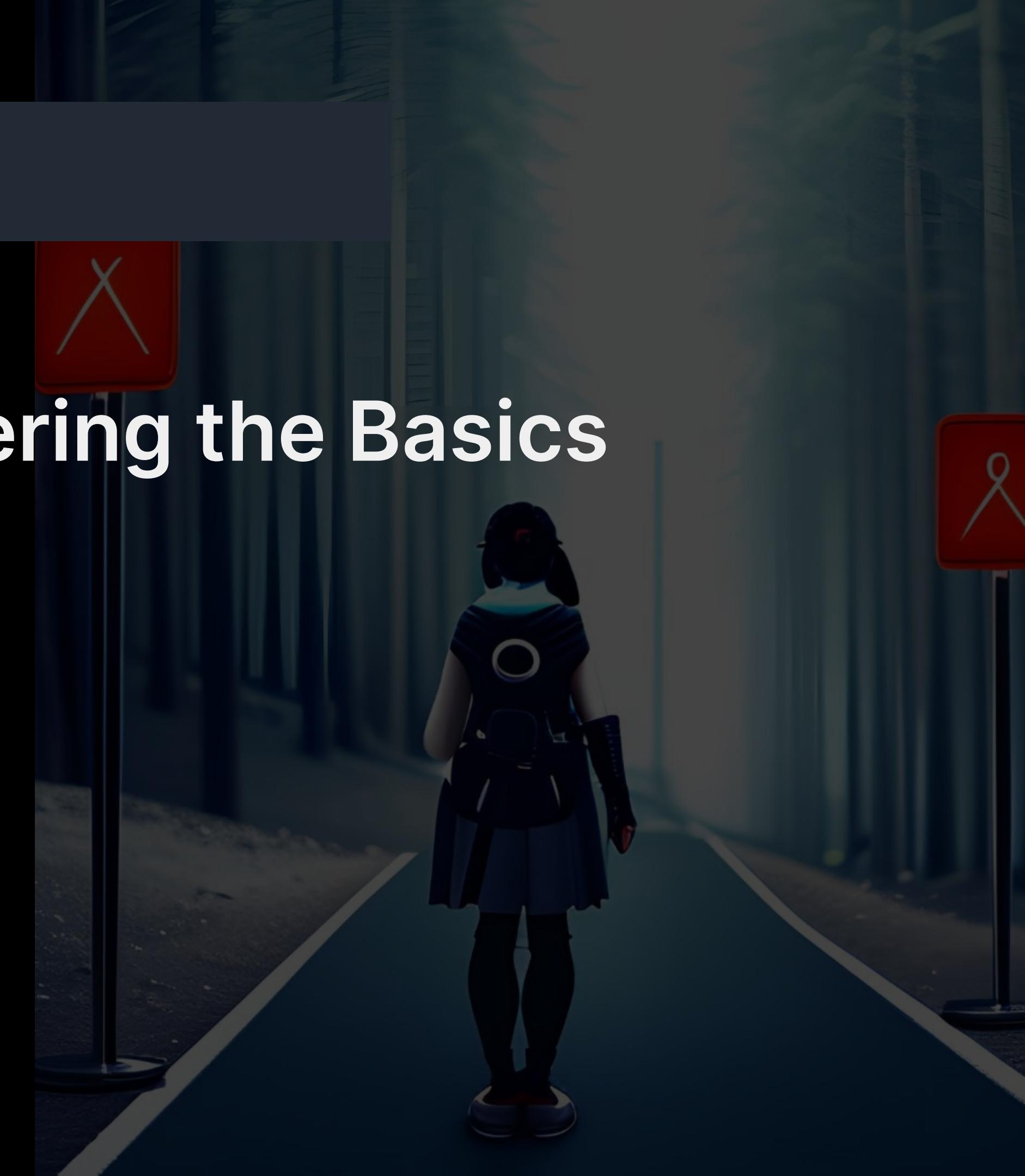
Takeaways

#1

Importance of Mastering the Basics

#2

#3



Takeaways

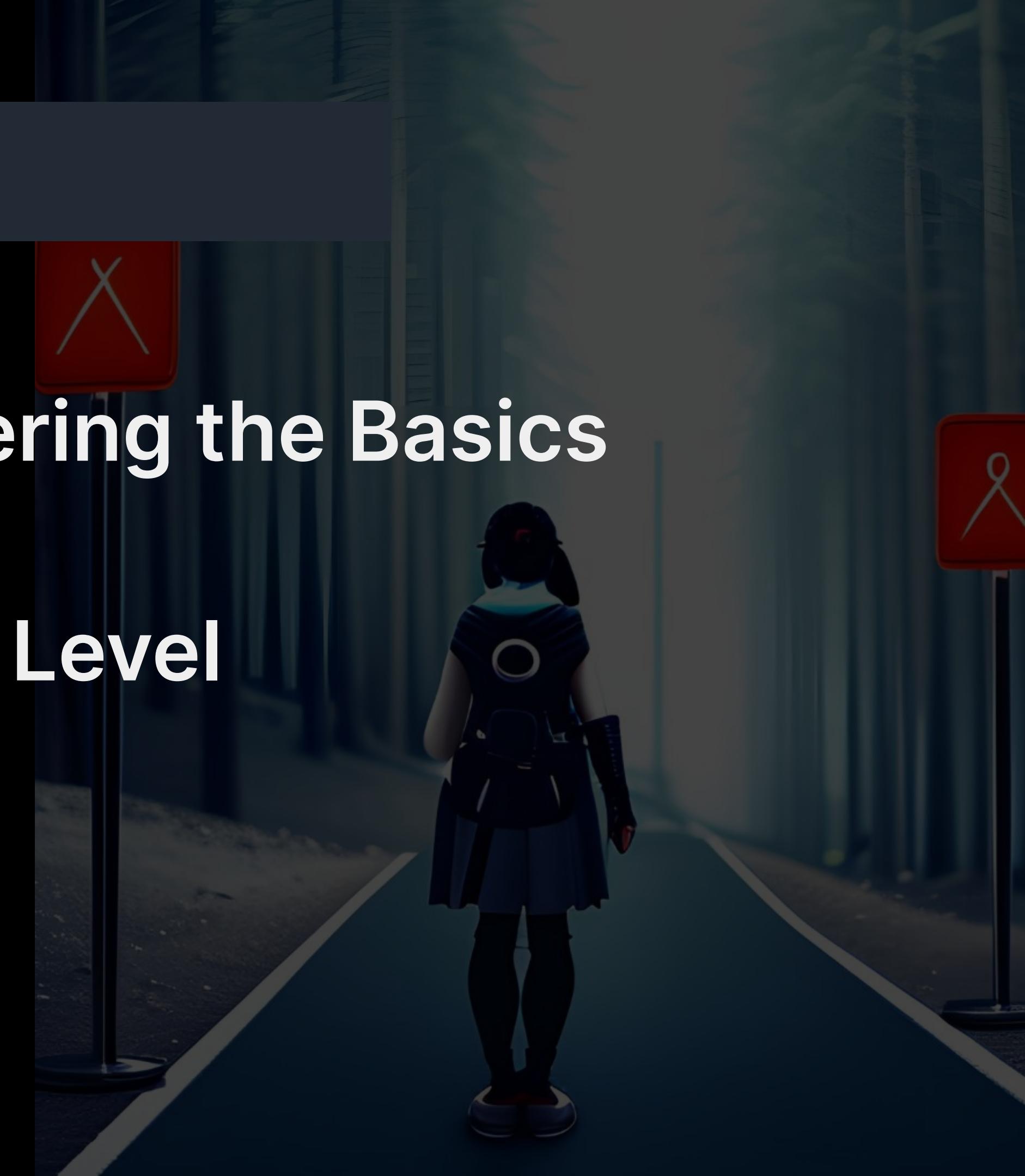
#1

Importance of Mastering the Basics

#2

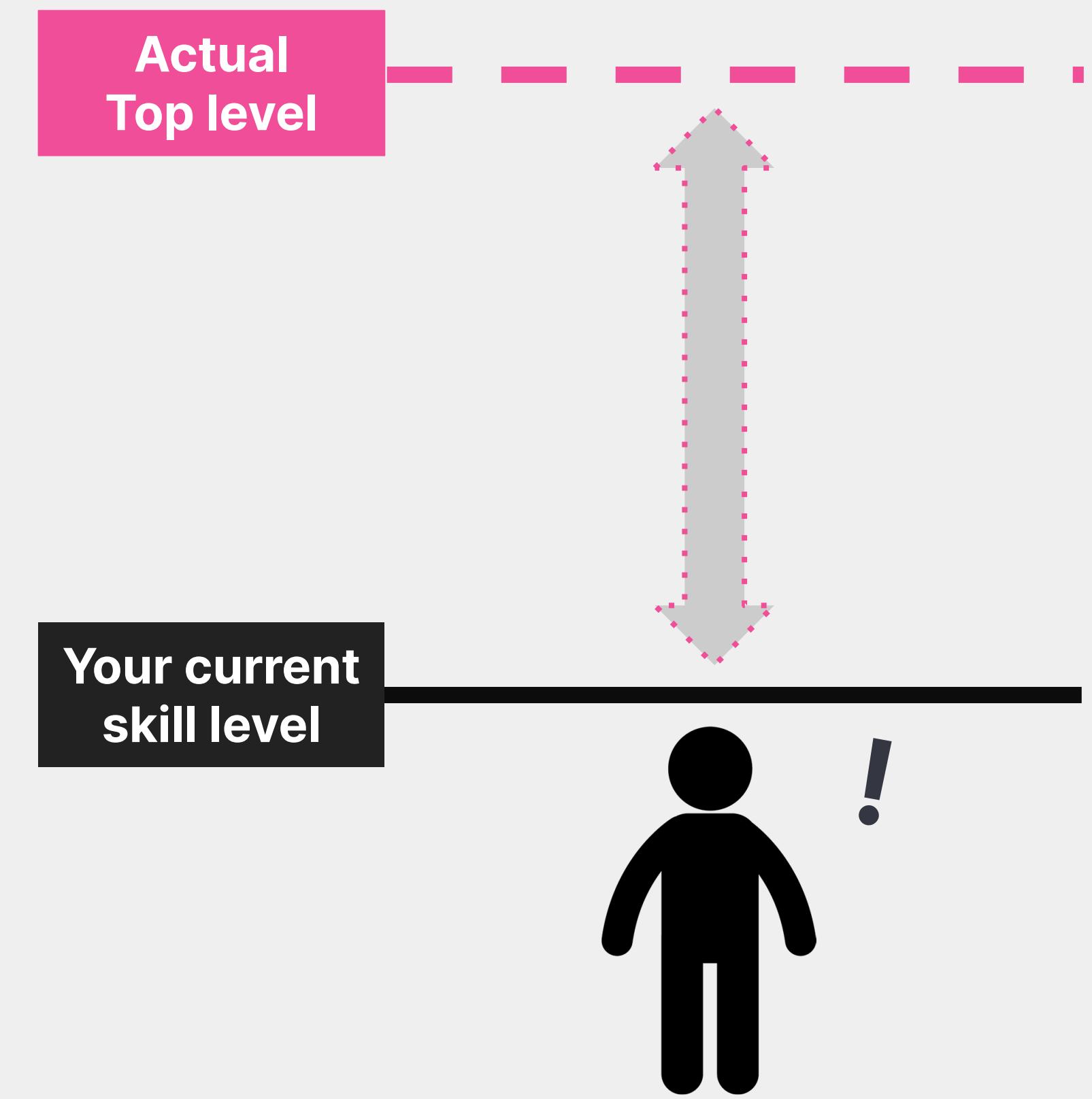
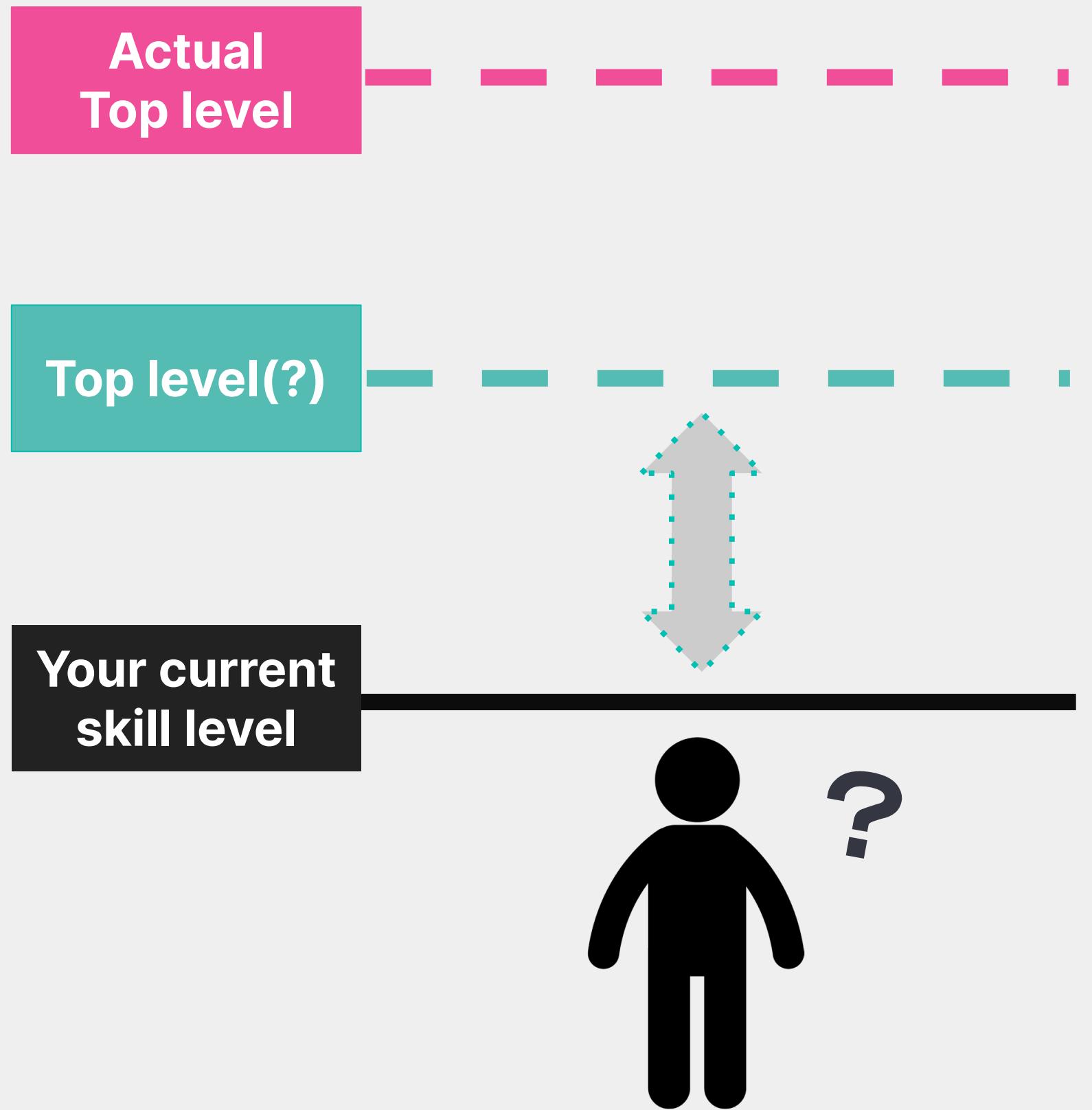
Understand the Top Level

#3



#2

Understand the Top Level



Takeaways

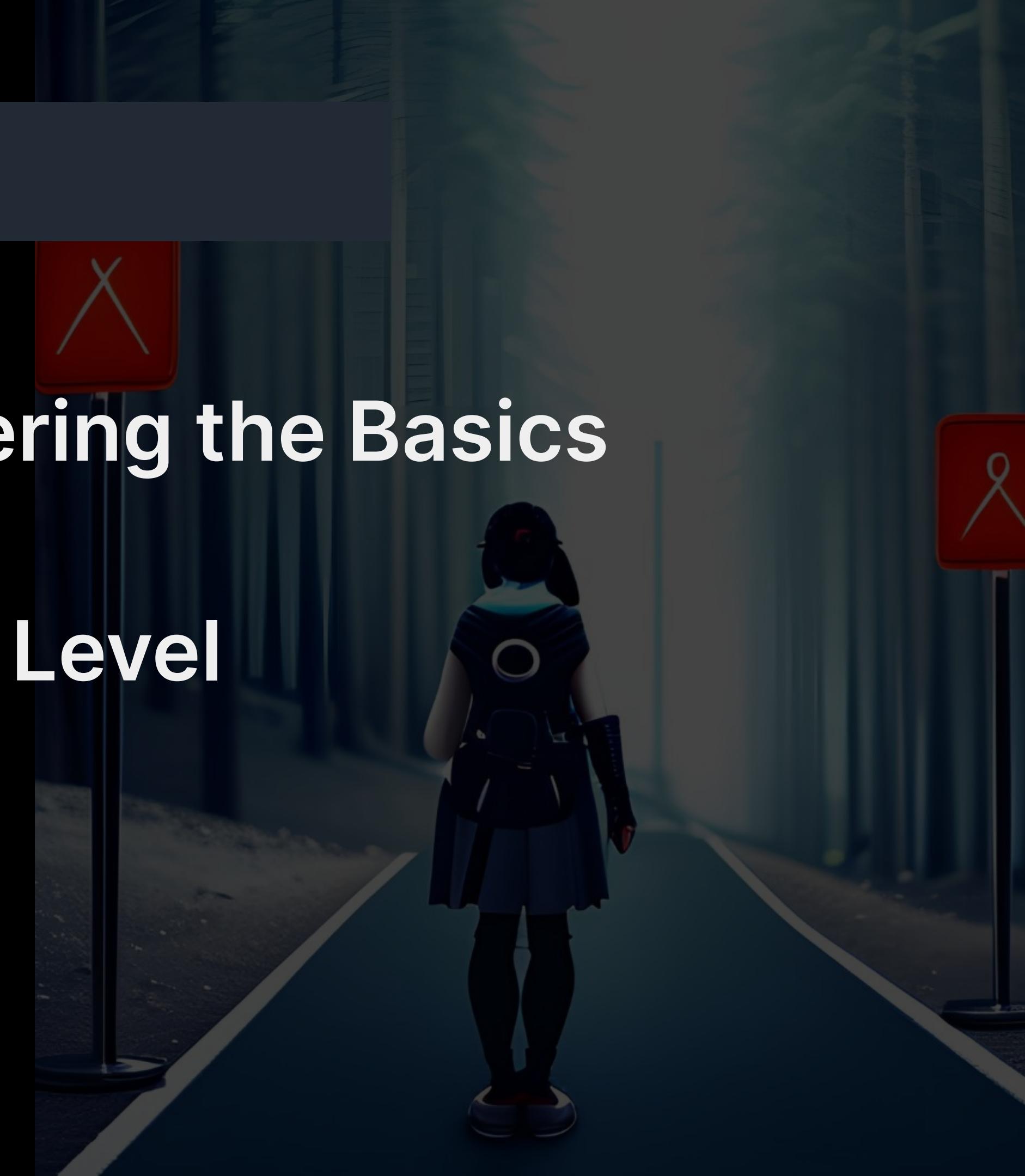
#1

Importance of Mastering the Basics

#2

Understand the Top Level

#3



Takeaways

#1

Importance of Mastering the Basics

#2

Understand the Top Level

#3

Keep in Mind that You Won't Succeed Easily

#3 Keep in Mind that You Won't Succeed Easily

Accepted at Black Hat!

Found a 0-Day!

What you see

Rejected again..

Couldn't find anything interesting..

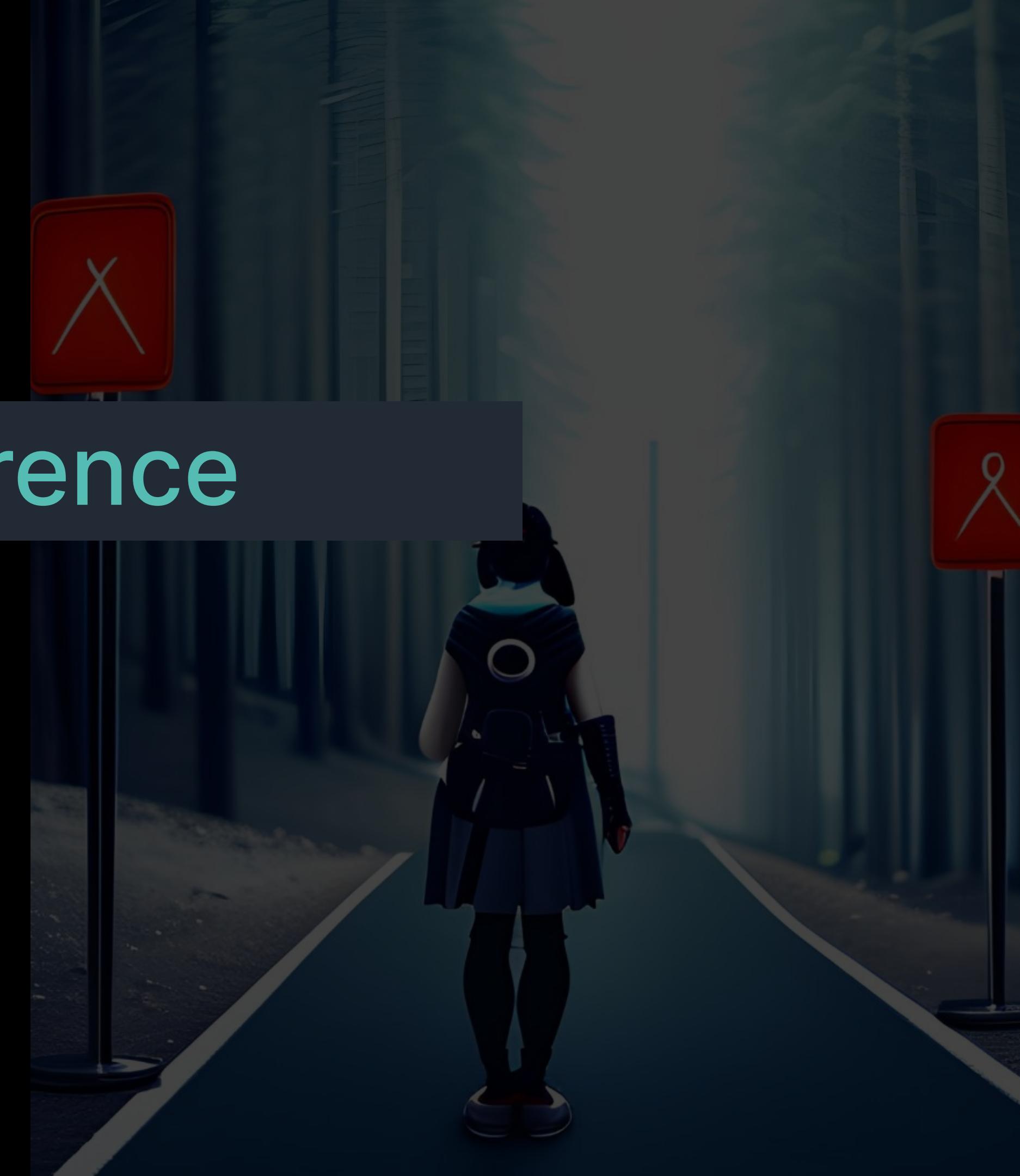


My program has a bug..



What you don't see

How to Make a Difference



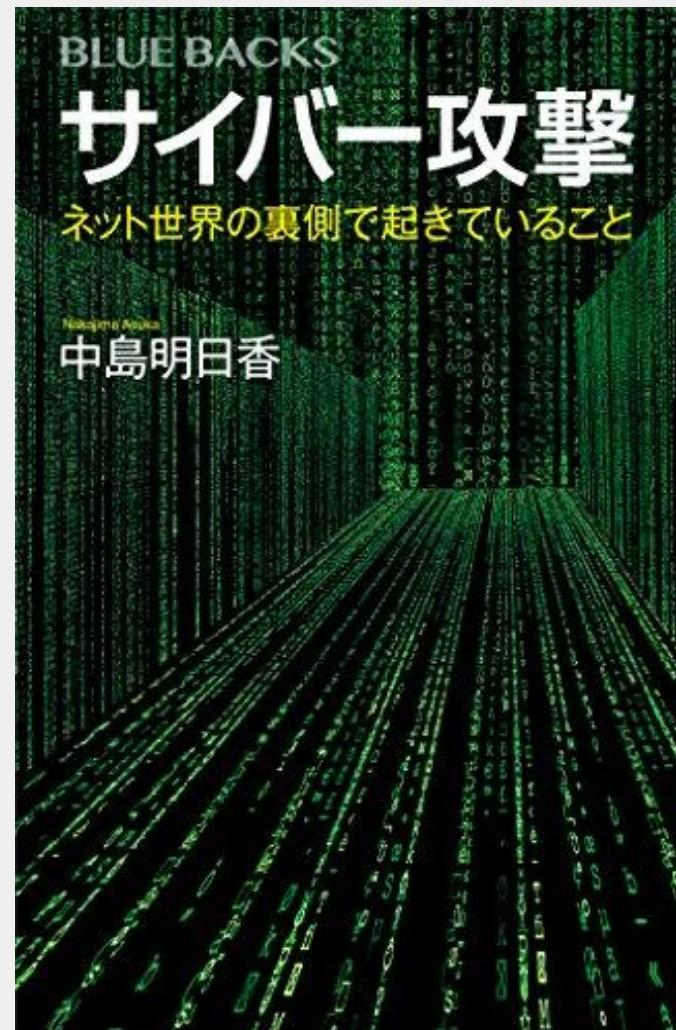
How to Make a Difference

How to Make a Difference

Always Keep in Mind What Value You Can Offer to Others

How to Make a Difference

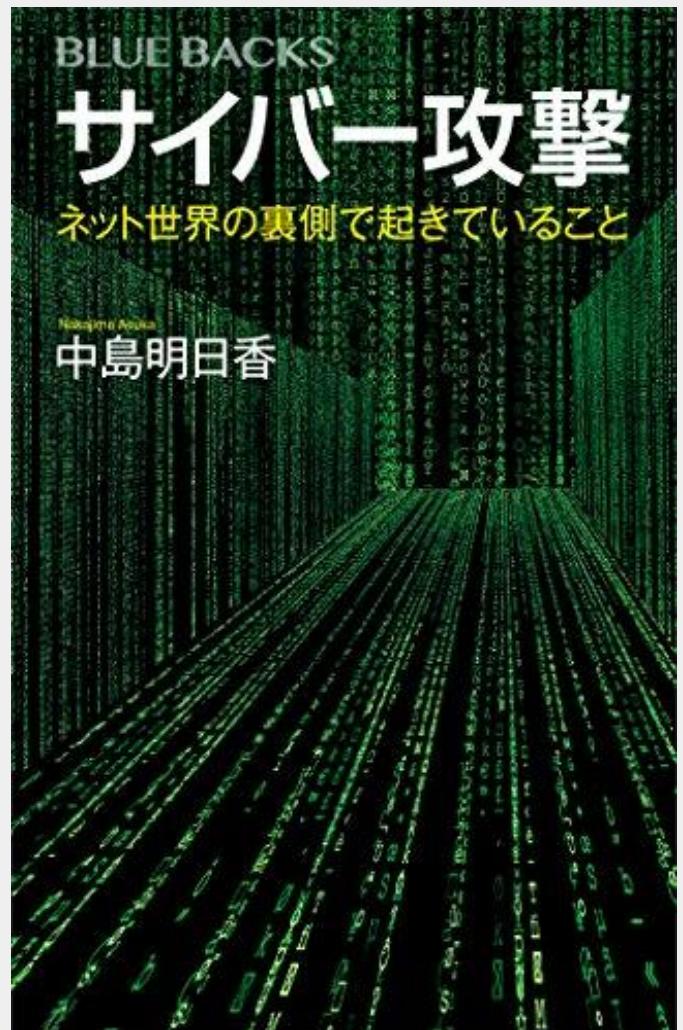
Always Keep in Mind What Value You Can Offer to Others



Talks about typical stack buffer overflow, but it became a best selling book. Why? 🤔

How to Make a Difference

Always Keep in Mind What Value You Can Offer to Others



Talks about typical stack buffer overflow, but it became a best selling book. Why? 🤔



There were no books written on such subjects for the general public 😲

How to Make a Difference

Always Keep in Mind What Value You Can Offer to Others



Example

**Can Provide Information about
Trends/Hot Topics in Japan**



Let's Make a Difference,
Starting from Here, Today !



Thank you for listening!

E-mail

asuka.nakajima@elastic.co

Website

<https://www.kunOichi.net/>

X(Twitter)

@AsuNa_jp

LinkedIn

<https://www.linkedin.com/in/asuka-nakajima-89493326/>

Facebook

<https://www.facebook.com/asuka.nakajima.9>